প্রশিক্ষণ নির্দেশিকা

ই-মেইল ও দলিলে ডিজিটাল স্বাক্ষর ব্যবহার

গণপ্রজাতন্ত্রী বাংলাদেশ সরকার

তথ্য ও যোগাযোগ প্রযুক্তি বিভাগ

ডাক, টেলিযোগাযোগ ও তথ্যপ্রযুক্তি মন্ত্রণালয়

প্রশিক্ষণ নির্দেশিকা

ই-মেইল ও দলিলে ডিজিটাল স্বাক্ষর ব্যবহার

সংস্করণ ১.২

ফেব্রুয়ারী, ২০১৪

প্রকাশকাল

১ম প্রকাশ জুন, ২০১২ খ্রিঃ

২য় প্রকাশ ফেব্রুয়ারী ২০১৪ খ্রিঃ

প্রকাশক

ইলেক্ট্রনিক নথি ব্যবস্থাপনায় ব্যবহারের জন্য সরকারী দপ্তর সমূহে ডিজিটাল স্বাক্ষর সার্টিফিকেট বিতরণ কর্মসূচী

এবং

ইলেক্ট্রনিক স্বাক্ষর সার্টিফিকেট প্রদানকারী কর্তৃপক্ষের নিয়ন্ত্রক এর কার্যালয়

সম্পাদনা

মোহাম্মদ এনামুল কবির

হাসান-উজ-জামান

জিয়াউদ্দিন আহমেদ

এ. কে. এম শাহাবুদ্দিন

মূদ্রণে ঃ

আউট লাইন প্রিন্টার্স

১৪৭/১ আরামবাগ, ঢাকা-১০০০

মোবাইল ঃ ০১৭১১৮৪২৮৯১

dotline.bd@gmail.com

সূচীপত্র

১. পটভূমি

দেশে ডিজিটাল স্বাক্ষর প্রবর্তন

ডিজিটাল বাংলাদেশ গঠনের অংশ হিসেবে আমাদের দেশে বিভিন্ন ক্ষেত্রে এখন ইলেক্ট্রনিক পদ্ধতি ব্যবহার করা হচ্ছে, যেমন: শিক্ষা প্রতিষ্ঠানে ভর্তি, ইলেক্ট্রিসিটি বিল প্রদান, রেলওয়ে টিকেট, পাসপোর্টের আবেদন, জেলা প্রশাসক অফিসের ই-সেবা, অনলাইন ট্যাক্স রিটার্ন, ইত্যাদি; কিন্তু এ সব ক্ষেত্রে যথাযথ নিরাপত্তা ব্যবস্থা গ্রহণ না করলে ব্যবহারকারির প্রতারিত হবার সম্ভাবনা থেকে যায়। ইলেক্ট্রনিক পদ্ধতির কার্যক্রমে নিরাপত্তা নিশ্চিতকরণে বিশ্বব্যাপী পরীক্ষিত ও স্বীকৃত প্রযুক্তি হল ডিজটাল স্বাক্ষর।

ডিজিটাল স্বাক্ষর প্রবর্তনে একটি দৃঢ় আইনি অবকাঠামো এবং নির্ভরযোগ্য কারিগরি অবকাঠামো প্রয়োজন। তথ্য ও যোগাযোগ প্রযুক্তি আইন ২০০৬ (সংশোধিত ২০১৩) এ ডিজিটাল স্বাক্ষরের আইনগত স্বীকৃতি দেয়া হয়েছে। সরকার প্রতিশ্রুত ডিজিটাল বাংলাদেশ বাস্তবায়নে প্রণীত জাতীয় তথ্য ও যোগাযোগ প্রযুক্তি নীতিমালা ২০০৯-এ ডিজিটাল স্বাক্ষর প্রবর্তনের নির্দেশনা দেয়া হয়। এ ব্যবস্থা প্রবর্তনে উক্ত আইন সংশোধনের প্রয়োজন দেখা দেয় এবং বাংলাদেশ কম্পিউটার কাউন্সিল তা সংশোধনের উদ্যোগ গ্রহণ করে। ২০০৯ সালে সরকার উক্ত আইনের প্রয়োজনীয় সংশোধনী অনুমোদন করে। এরপর ডিজিটাল স্বাক্ষর প্রবর্তনে বিভিন্ন প্রস্তুতিমূলক কার্যক্রম বাস্তবায়ন শুরু হয়।

সিসিএ কার্যালয় সংগঠন

ডিজিটাল স্বাক্ষরসহ সাইবার নিরাপত্তা বিধানে বিভিন্ন কার্যক্রম যার তত্ত্বাবধানে পরিচালিত হয় তিনি কন্ট্রোলার অফ সার্টিফাইং অথরিটিজ বা সিসিএ। সিসিএ কার্যালয় সংগঠনের প্রথম যা প্রয়োজন ছিল তা হলোঃ (১) জনবল ও (২) বাজেট। জনবলের জন্য বিসিসি হতে প্রথমে ১০১ জন জনবলের একটি অর্গানোগ্রামসহ খসড়া চাকুরী প্রবিধানমালা ১০-০১-২০১০ তারিখ প্রস্তাব করা হয়। এরপর তৎকালিন সংস্থাপন মন্ত্রণালয় হতে "সিসিএ কার্যালয় প্রকৃতি কি হবে" সে প্রশ্ন উত্থাপিত হয়। প্রথমে এটি বিসিসি'র অধীন একটি প্রতিষ্ঠান চিন্তা করা হয়েছিল। পরবর্তীতে মে ২০১১ মাসে সিসিএ কার্যালয়কে মন্ত্রণালয়ের একটি সংযুক্ত দপ্তর হিসেবে ঘোষনা করা হয়। এর আগে সরকার এপ্রিল ২০১১ মাসে এ কার্যালয়ের জন্য ৩৫ জনবলের একটি কাঠামো অনুমোদন করে। জুন ২০১২ মাসে সিসিএ কার্যালয়ের চাকুরী বিধিমালা/ প্রবিধানমালা চুড়ান্ত হয়।

সার্টিফাইং অথরিটি লাইসেন্সিং

সার্টিফাইং অথরিটি বা সিএ লাইসেন্স প্রদানের পূর্বে লাইসেন্সিং ফি, নবায়ন ফি, আগ্রহী প্রতিষ্ঠানের পরিশোধিত মূলধনের পরিমান, ইত্যাদি আর্থিক বিষয়ে সিদ্ধান্তের জন্য অর্থ বিভাগে প্রস্তাব পেশ করা হয়। এ বিষয়ে অর্থ বিভাগের সিদ্ধান্ত পাবার পর ১৯ জানুয়ারী ২০১১ তারিখ ৬টি দেশীয় প্রতিষ্ঠান যথাক্রমে ম্যাংগো টেলিসার্ভিসেস লিঃ, বাংলা ফোন লিঃ, ফ্লোরা টেলিকম, ডাটা এজ লিঃ, কম্পিউটার সার্ভিসেস লিঃ এবং দোহাটেক নিউ মিডিয়া- কে সার্টিফাইং অথরিটি হিসেবে লাইসেন্স প্রদান করা হয়। পরবর্তীতে বিভিন্ন শ্রেণীর ডিজিটাল সার্টিফিকেটের ফি নির্ধারণে লাইসেন্স প্রাপ্ত প্রতিষ্ঠানগুলোর নিকট হতে প্রস্তাব আহ্বান করা হয়। প্রাপ্ত ফি প্রস্তাব এবং পার্শ্ববর্তী বিভিন্ন দেশের বিদ্যমান ফি পর্যালোচনা করে বিভিন্ন শ্রেণীর সার্টিফিকেট ফি এর সর্বোচ্চ সীমার একটি তালিকা ৯ জুন ২০১১ তারিখে সিসিএ কর্তৃক গণবিজ্ঞপ্তি আকারে প্রকাশ করা হয়। ২০১৪ সালের জানুয়ারী মাসে বাংলাদেশ কম্পিউটার কাউন্সিল (বিসিসি)-কে সরকারী পর্যায়ে কার্যক্রম পরিচালনার জন্য সিএ লাইসেন্স প্রদান করা হয়।

রুট কী জেনারেশন সিরিমনি

উল্লিখিত প্রস্তুতিমূলক কার্যক্রম সম্পন্ন করার সুবাদে দেশে ডিজিটাল স্বাক্ষর প্রবর্তনের পথ সুগম হয়। ১৮ এপ্রিল ২০১২ তারিখে রুট কী জেনারেশন সিরিমনি অনুষ্ঠিত হয়। এ অপরিহার্য ধাপ সম্পন্ন হবার পর কারিগরিভাবে প্রস্তুত ও অডিট সম্পন্ন হওয়া নিম্নোক্ত ৩টি সিএ প্রতিষ্ঠানকে বাণিজ্যিকভাবে দেশে ডিজিটাল স্বাক্ষর ব্যবহারের অনুমতি দেওয়া হয় এবং প্রতিষ্ঠান ৩টি বর্তমানে গ্রাহক পর্যায়ে সার্টিফিকেট প্রদান করেছে।

1. Mango Teleservices Ltd.
   Web: www.mango.com.bd
2. Dohatec new media
   Web: www.dohatec.com
3. Data Edge Limited
   Web: www.data-edge.com

২৮ নভেম্বর ২০১৩-তারিখে রুট সিএ'র সার্টিফিকেটে object Identifier (OID) সংযুক্ত করে নতুন রুট কী জেনারেশন করা হয়েছে। তাছাড়া ৫ টি সিএ প্রতিষ্ঠানের অনুকূলে সিসিএ কর্তৃক (OID) বরাদ্দ করা হয়েছে। উল্লেখ্য রুট সিএ'র সার্টিফিকেট বাংলাদেশের একমাত্র স্ব-স্বাক্ষরিত সার্টিফিকেট। অন্য সকল সিএ'র সার্টিফিকেট রুট সিএ দ্বারা স্বাক্ষরিত।

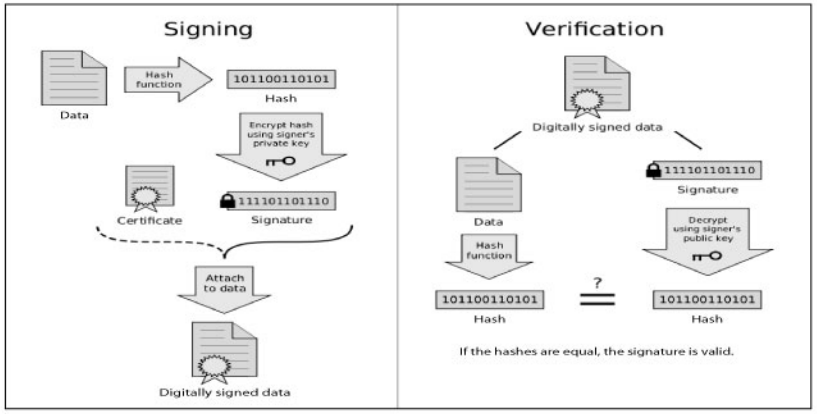
কর্মশালা ও অবহিতকরণ কর্মসূচি

ডিজিটাল স্বাক্ষর প্রবর্তনে সরকার কর্তৃক বিভিন্ন পদক্ষেপের মধ্যে অন্যতম হচ্ছে সাধারণ মানুষের মধ্যে এ ব্যাপারে সচেতনতা সৃষ্টি করা। এ ক্ষেত্রে প্রশিক্ষণ, কর্মশালা, সেমিনার এবং মতবিনিময় সভার আয়োজন করা হয়েছে এবং ভবিষ্যতে আরো ব্যাপক আকারে এ সমস্ত কর্মসূচি আয়োজনের পরিকল্পনা রয়েছে। এ সকল অনুষ্ঠানে অংশগ্রহকারীদের জন্য একটি নির্দেশনা সম্বলিত পুস্তিকা বা ম্যানুয়াল দরকার। অংশ্রহণকারীরা পরে তা ব্যবহার করে নিজেরা ডিজিটাল স্বাক্ষরের ব্যবহারিক বিষয়ে অনুশীলন করতে পারবেন এবং অন্যদেরকে প্রশিক্ষন দিতে পারবেন। এ পুস্তিকায় ডকুমেন্ট ও মেইল কিভাবে ডিজিটাল স্বাক্ষরযুক্ত করা যায়, কিভাবে মেইল এনক্রিপ্ট করে পাঠাতে হয় ইত্যাদি বিষয়াদি বিস্তারিত বর্ণনা করা হয়েছে। আশা করা যায় যে, এ পুস্তিকাটি ডিজিটাল স্বাক্ষর বিষয়ে শিক্ষার্থী ও ব্যবহারকারীদের প্রয়োজন মিটাতে সহায়ক হবে।

২. ডিজিটাল স্বাক্ষর কিভাবে কাজ করে

ডিজিটাল স্বাক্ষর হল ইলেকট্রনিক পদ্ধতিতে তথ্য বিনিময়ের ক্ষেত্রে তথ্য প্রদানকারির পরিচয় যাচাইয়ের একটি পন্থা। এটি নিশ্চিত করে যে তথ্যটি যিনি পাঠিয়েছেন তার সেটি পাঠানোর কর্তৃত্ব আছে (তিনি নিজে) এবং যাত্রাপথে এ তথ্যে কোন পরিবর্তন ঘটেনি। সাধারনতঃ ইন্টারনেট বা নেটওয়ার্কে আর্থিক লেনদেন বা অন্য কোন গোপণীয় লেনদেনের ক্ষেত্রে এর সঙ্গে ডিজিটাল স্বাক্ষর জুড়ে দেওয়া হয়। ডিজিটাল স্বাক্ষর প্রয়োগের জন্য ডিজিটাল সনদ প্রয়োজন। ডিজিটাল সনদ হল তথ্যে বিনিময়ের ক্ষেত্রে দাতা কিংবা গ্রহীতা অথবা উভয় প্রান্তে ব্যবহৃত নিরাপত্তা নিশ্চিতকরণের একটি ইলেকট্রনিক প্রত্যয়ণ ব্যবস্থা। এটি বিশ্বব্যাপি পরিক্ষীত ও স্বীকৃত।

ডিজিটাল স্বাক্ষর সংযুক্ত করতে প্রথমেই দলিল বা ডকুমেন্টকে একটি জটিল সংখ্যায় পরিণত করা হয় যা উক্ত দলিল বা ডকুমেন্টের জন্য অনন্য। এই জটিল গাণিতিক সংখ্যাটিকে বলা হয় হ্যাশ ফাংশন। একটি বিশেষ এলগরিদমের সাহায্যে একজোড়া (জটিল) গাণিতিক সংখ্যা তৈরি করা হয়। এ সংখ্যা জোড়া পরস্পর এমনভাবে সম্পর্কযুক্ত যে, একটি থেকে অপরটি কখনো বের/অনুমান করা যায় না। কিন্তু বিশেষ পদ্ধতিতে দুইটি আলাদাভাবে ব্যবহার করে একই ফল পাওয়া যায়। এ সংখ্যা দু'টি চাবি (কী) নামে পরিচিত। হ্যাশ এবং কী এর সমন্বয়ে তৈরি হয় ডিজিটাল স্বাক্ষর ও প্রমাণীকরণ ব্যবস্থা।



সাধারনতঃ প্রতিটি ডিজিটাল সার্টিফিকেট/সনদ এর সাথে দু'টি কী বা চাবি থাকে এর একটি প্রাইভেট কী (নিজের গোপণীয় চাবি) এবং অপরটি পাবলিক কী (সবার জন্য উন্মোচনের চাবি)। প্রেরক যে দলিল পাঠাবেন তার একটি হ্যাশ তৈরি করা হয়, তারপর গোপণীয় চাবি (প্রাইভেট কী) দিয়ে সেই হ্যাশটিকে একটি অনন্য রূপে [ডিজিটাল স্বাক্ষর] পরিণত করা হয়। কম্পিউটার প্রোগ্রাম দিয়ে এ কাজগুলো করা হয়। তারপর দলিল ও স্বাক্ষর দুটোই প্রাপকের কাছে পাঠিয়ে দেয়া হয়। প্রাপকের কম্পিউটারে প্রথমে একই নিয়মে প্রাপ্ত দলিলকে হ্যাশে পরিণত করেন আর প্রেরকের পাবলিক কী দিয়ে স্বাক্ষর থেকেও হ্যাশ বের করেন। দু'টি হ্যাশ এক হলে সনাক্তকরণ নিশ্চিত হয়। এবং তা প্রমাণ করে যে প্রেরিত দলিলটি যথার্থই প্রেরক কর্তৃক প্রেরিত এবং তথ্যে কোন পরিবর্তন ঘটেনি।

৩. ডিজিটাল স্বাক্ষর সার্টিফিকেটের ব্যবহার

ডিজিটাল স্বাক্ষর সার্টিফিকেটের বহুবিধ ব্যবহার রয়েছে। মূলত: ই-গভর্নেন্স এ্যাপ্লিকেশন্স, ই-লেনদেন, ই-কমার্স, ই-প্রকিউরমেন্ট, অনলাইন ব্যাংকিং, ইলেকট্রনিক যোগাযোগ ইত্যাদি ক্ষেত্রে ডিজিটাল স্বাক্ষর সার্টিফিকেট ব্যবহার করা হয়। এক কথায় বলা যায়, যে সকল ক্ষেত্রে পরিচিতি প্রতিপাদন প্রয়োজন, যে সকল ইলেকট্রনিক যোগাযোগ বা লেনদেনের ক্ষেত্রে নিরাপত্তা প্রয়োজন সেই সকল ক্ষেত্রে ডিজিটাল স্বাক্ষর সার্টিফিকেট ব্যবহার করা হয়ে থাকে। এই নির্দেশিকার পরবর্তী অংশগুলোতে কিভাবে ডিজিটাল স্বাক্ষর সার্টিফিকেট ব্যবহার করে একটি ডকুমেন্ট স্বাক্ষর করা যায়, কিভাবে ই-মেইল স্বাক্ষর করা যায় এবং ই-মেইল এনক্রিপ্ট করা যায় তা দেখানো হয়েছে। মাইক্রোসফট উইন্ডোজ অপারেটিং সিস্টেম, লিনাক্সের উবুন্টু অপারেটিং সিস্টেম উভয় ক্ষেত্রেই ডকুমেন্ট স্বাক্ষর এবং ই-মেইল স্বাক্ষর ও এনক্রিপশন দেখানো হয়েছে।

সার্টিফিকেট প্রদানকারী কর্তৃপক্ষ (সিএ) গ্রাহক পর্যায়ে ডিজিটাল স্বাক্ষর সার্টিফিকেট ইস্যু করবে। ডিজিটাল স্বাক্ষর সার্টিফিকেট দুই ভাবে গ্রহণ করা য়ায়, (ক) সফট টোকেনের মাধ্যমে এবং (খ) হার্ড/ক্রিপ্টো টোকেনের মাধ্যমে। এই দুই পদ্ধতির ক্ষেত্রে কিভাবে ডিজিটাল স্বাক্ষর সার্টিফিকেট ব্যবহার করে ডকুমেন্ট স্বাক্ষর এবং ই-মেইল স্বাক্ষর ও এনক্রিপশন করা যায় তা পরবর্তীতে দেখানো হয়েছে।

৩.১ নির্দেশিকার ব্যবহারিক অংশে ব্যবহৃত হার্ডওয়্যার ও সফটওয়্যার

- অপারেটিং সিস্টেম ঃ উইন্ডোজ এক্সপি, উবুন্টু লিনাক্স ১০.০৪
- ডকুমেন্ট এডিটর ঃ মাইক্রোসফট অফিস এক্সপি, ওপেন অফিস ৩.২, অ্যাডোব অ্যাক্রোব্যাট প্রফেশনাল ৬.০
- মেইল ক্লায়েন্টঃ মাইক্রোসফট আউটলুক এক্সপি, এভোলুশন ২.২৮.৩
- ই-টোকেন

৪. ডিজিটাল স্বাক্ষর ব্যবহার পদ্ধতি

৪.১ ডিজিটাল স্বাক্ষর সার্টিফিকেটের ব্যবহার পদ্ধতি (সফট টোকেন)

সফ্‌ট টোকেনের মাধ্যমে অথবা ফাইল হিসেবে প্রাপ্ত সার্টিফিকেট দ্বারা ডিজিটাল স্বাক্ষর প্রয়োগের পূর্বে নিম্নলিখিত প্রস্তুতি সম্পন্ন করতে হবে।

(ক) প্রথমে আপনাকে একজন বৈধ সার্টিফিকেট প্রদানকারী কর্তৃপক্ষ (Certifying Authority) এর কাছ থেকে আপনার ডিজিটাল স্বাক্ষর সার্টিফিকেট সংগ্রহ করতে হবে।

(খ) এজন্য সিএ'র নির্দেশিত ফরম পূরণ করে আপনাকে সেটি জমা দিতে হবে, আপনার "কী-পেয়ার" (key-Pair) তৈরি করার সময় আপনাকে একটি পাসওয়ার্ড/পাস-ফ্রেজ (Pass-Phrase) দিতে হবে। পাসওয়ার্ড/পাস-ফ্রেজ একান্ত ব্যক্তিগত এবং গোপণীয়। সুতরাং তা যথাযথভাবে সংরক্ষণ করতে হবে।

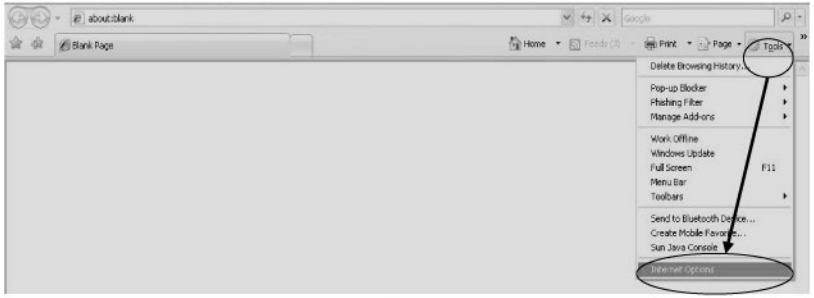
(গ) সিএ আপনার "কী" জেনারেট করার পর আপনাকে সার্টিফিকেটসহ সেটি হস্তান্তর করবে। আপনি ডাউনলোড করে সেটি ফাইল হিসেবে গ্রহণ করতে পারেন অথবা ক্রিপ্টো টোকেনের মধ্যেও সেটি গ্রহণ করতে পারেন। ফাইল হিসেবে গ্রহণের ক্ষেত্রে আপনি <Name>. p12 অথবা <Name>. pfx (ব্যবহারকারীর প্রাইভেট কীসহ সার্টিফিকেট) শীর্ষক একটি ফাইল পাবেন।

৪.১.১ উইন্ডোজ অপারেটিং সিস্টেমে ডিজিটাল স্বাক্ষর ব্যবহার

উইন্ডোজ অপারেটিং সিস্টেমের নির্ধারিত (default) ব্রাউজার হল Internet Explorer। Internet Explorer এ সার্টিফিকেট ইনস্টল করলে তা অপারেটিং সিস্টেম এর সার্টিফিকেট ভান্ডারে (store) সংযুক্ত হয়ে যাবে। সুতরাং আপনার ব্যক্তিগত (Personal) সার্টিফিকেট এবং সিএ সার্টিফিকেটটি Internet explorer এ import করুন। এরপর আপনি ডিজিটাল স্বাক্ষর প্রয়োগ করতে পারবেন।

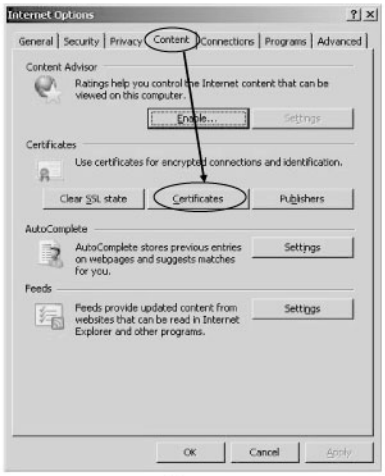
(ক) ইন্টারনেট এক্সপ্লোরারের জন্য ব্যক্তিগত সার্টিফিকেট 'Import' করার পদ্ধতি

IE (Internet Explorer) চালু করুন। নিচের চিত্রে চিহ্নিত 'Tools' লেবেলের উপর ক্লিক করুন। একটি ড্রপ ডাউন মেনু খুলবে। মেনুতে 'Internet Options' এ ক্লিক করুন (চিত্র-১)।



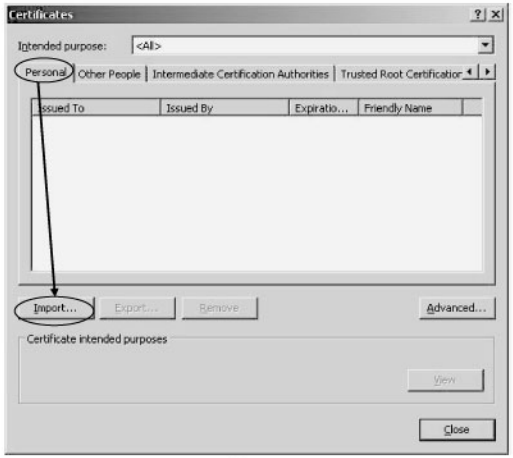
চিত্র-১

ফলে একটি ডায়ালগ বক্স (চিত্র-২) আসবে। এখানে বেশ কিছু ট্যাব দেখা যাবে। চিত্র-২ এ চিহ্নিত 'Content' ট্যাবে ক্লিক করুন। ফলে যে পেইজটি দেখা যাবে, তার মাঝামাঝি স্থানে অবস্থিত 'Certificates' বাটনটিতে ক্লিক করুন।



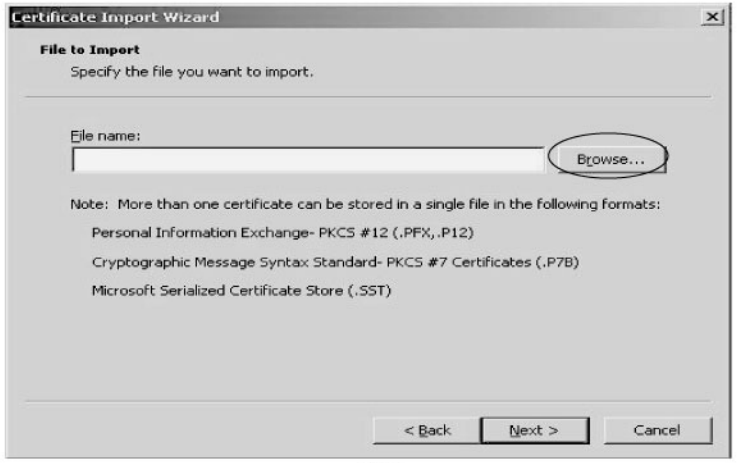
চিত্র-২

Certificates নামে আরেকটি নতুন ডায়ালগ বক্স (চিত্র-৩) আসবে। এখানে 'Personal' ট্যাব সহ বেশ কিছু ট্যাব দেখা যাবে। একজন গ্রাহকের ব্যক্তিগত সার্টিফিকেট 'Personal' ট্যাবে 'Import' করতে হয়। 'Personal' ট্যাব পেইজটিতে 'Import' নামে বাটনটিতে ক্লিক করুন।



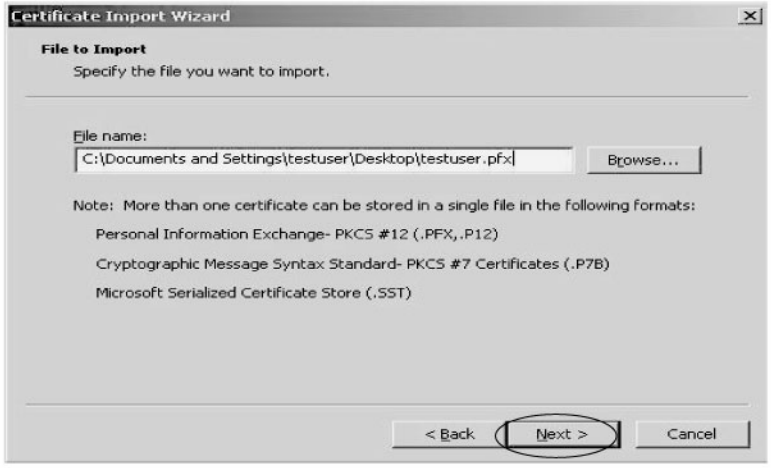
চিত্র-৩

ক্লিক করার পর একটি উইজার্ড চালু হবে (চিত্র-৪)। উইজার্ডটিতে প্রথমে আপনার ব্যক্তিগত সার্টিফিকেটটি খুঁজে (browse) দেখিয়ে দিতে হবে। এ জন্য চিত্র-৪ এ চিহ্নিত 'Browse' বাটনটিতে ক্লিক করুন এবং আপনার সার্টিফিকেটটি (pfx/p12 extension সহ) কম্পিউটারে যেখানে আছে, সেখান থেকে নির্বাচন করুন।



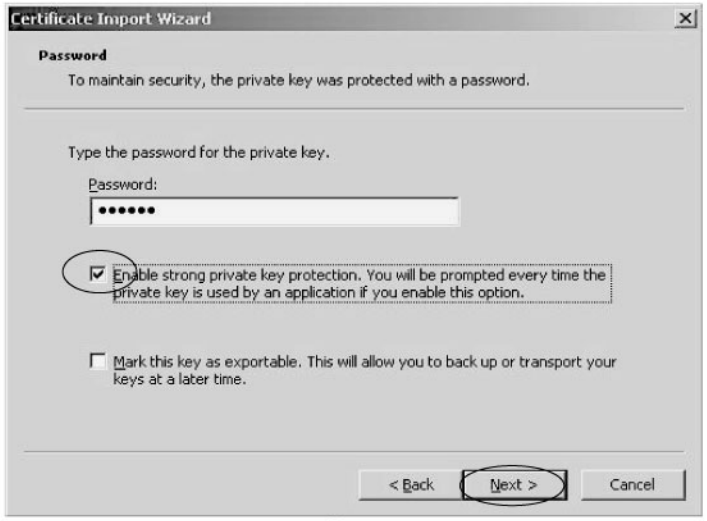
চিত্র-৪

ফলে চিত্র-৫ এর টেক্সট বক্সে আপনার সার্টিফিকেট ফাইলটির নাম দেখা যাবে। এবার Next বাটন চাপুন।



চিত্র-৫

Next বাটন ক্লিক করার পর আপনার কাছে export/import এর জন্য পাসওয়ার্ড চাইবে (চিত্র-৬)। এটি একটি নিরাপত্তা ব্যবস্থা। আপনার পাসওয়ার্ডটি লিখুন। চিত্র-৬ এ গোলাকার চিহ্নিত "Enable Strong Private Key Protection" অপশনে ক্লিক করুন। অতঃপর Next বাটন চাপুন।



চিত্র-৬

Next বাটন ক্লিক করার পর 'Certificate Store' নামে একটি পেইজ (চিত্র-৭) দেখাবে। এখানে কোন কিছু পরিবর্তনের দরকার নেই। 'Next' বাটনে ক্লিক করুন।

চিত্র-৭

এ পর্যায়ে যে ধাপগুলি পার করে এসেছেন তার একটি সংক্ষিপ্তসার (Summary) দেখা যাবে (চিত্র-৮)। অতঃপর 'Finish' বাটন চাপুন।

চিত্র-৮

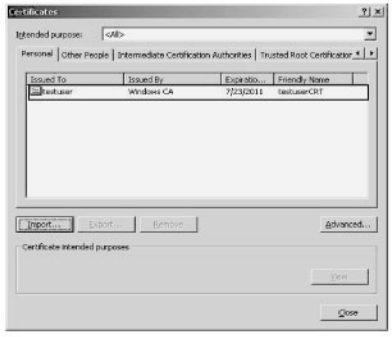
ফলে আপনাকে একটি বার্তা (চিত্র-৯) দেখাবে যে একটি নতুন প্রাইভেট কী import হচ্ছে। ok বাটন চাপুন।

চিত্র-৯

ফলে সফলভাবে একটি নতুন সার্টিফিকেট import হবে এবং এ সংক্রান্ত একটি সফলবার্তা (চিত্র-১০) দেখাবে। Ok বাটনে ক্লিক করুন।

চিত্র-১০

আপনি এখন ফিরে আসলেন Certificates ডায়ালগ বক্সের Personal ট্যাব পেইজটিতে। এখানে imported certificates এর status দেখতে পাবেন (চিত্র-১১)।

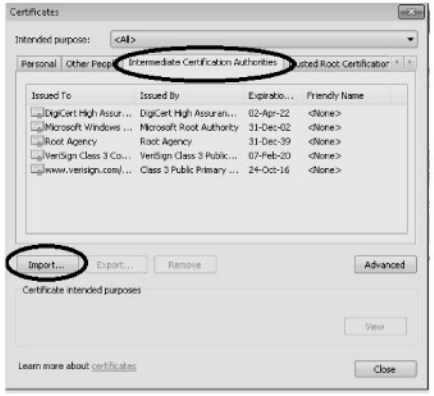


চিত্র-১১

(খ) ইন্টারনেট এক্সপ্লোরারের জন্য সিএ সার্টিফিকেট 'import' করার পদ্ধতি

বাংলাদেশে যে সকল সিএ প্রতিষ্ঠান থেকে গ্রাহকরা সার্টিফিকেট গ্রহণ করবেন, সে সকল সিএ প্রতিষ্ঠানসমূহ গ্রাহকদের নিকট চেইন সার্টিফিকেট প্রদান করবে অর্থাৎ গ্রাহকের সার্টিফিকেটের সাথে সিএ'র নিজের সার্টিফিকেটও থাকবে। ফলে গ্রাহকের সার্টিফিকেট ইনস্টল হলে স্বয়ংক্রিয়ভাবে সিএ সার্টিফিকেটও ইনস্টল হয়ে যাবে। আলাদাভাবে সিএ সার্টিফিকেট ইনস্টল করতে হবে না। তথাপি ব্যবহারকারীদের সুবিধার্থে নিম্নে সিএ সার্টিফিকেট ইনস্টল পদ্ধতি দেখানো হল।

ব্যক্তিগত সার্টিফিকেট import এর মত করে একইভাবে সিএ সার্টিফিকেটটি internet explorer এ import করতে হয়। ধরা যাক, আপনি Certificates ডায়ালগ বক্সের Personal ট্যাবে আছেন। এবার ডানদিকে "Intermediate Certifcation Authorities" ট্যাবটিতে (চিত্র-১২) ক্লিক করুন।

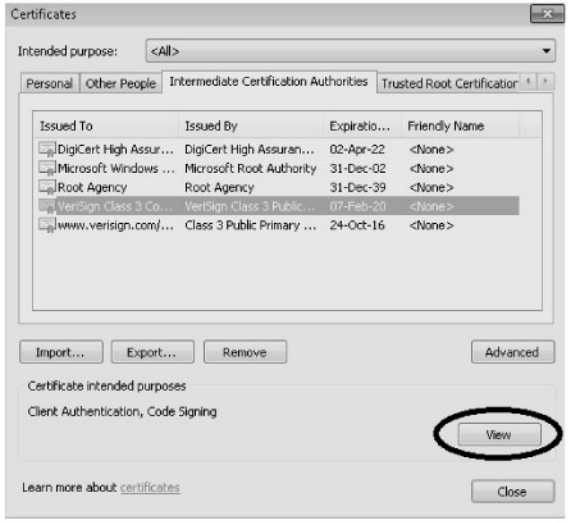


চিত্র-১২

যে পেইজটি খুলবে, সেখানে import বাটনে ক্লিক করে আগের পদ্ধতির (যেভাবে ব্যক্তিগত সার্টিফিকেট import করেছিলেন) ধাপগুলো অনুসরণ করুন। অবশেষে আপনাকে একটি warning message (চিত্র-১৩) দেখাবে যে আপনি সিএ কে trust করেন কিনা। নিশ্চিতকরণের জন্য Yes বাটন চাপুন।

চিত্র-১৩

"Intermediate Certifcation Authorities" ট্যাবটিতে আপনি সার্টিফিকেটের status (চিত্র-১৪) দেখতে পাবেন।



চিত্র-১৪

আপনি যদি সার্টিফিকেটের বিস্তারিত দেখতে চান তাহলে সিএ সার্টিফিকেটটি নির্বাচন করুন এবং View বাটনে (চিত্র-১৪) ক্লিক করুন। তখন সার্টিফিকেটের তথ্য সম্বলিত একটি পেইজ (চিত্র-১৫) খুলবে যেখানে সার্টিফিকেটটির বিস্তারিত তথ্য দেখা যাবে।

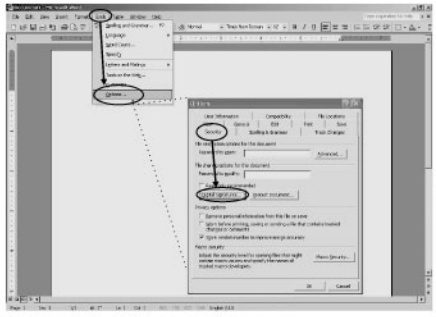
চিত্র-১৫

একই পদ্ধতিতে Trusted Root Certification Authorities ট্যাবে ক্লিক করে বাংলাদেশের রুট সার্টিফিকেট ইমপোর্ট করে নিতে হবে। www.cca.gov.bd ওয়েবসাইট থেকে রুট সিএ'র সার্টিফিকেট ডাউনলোড করা যাবে।

(গ) ডকুমেন্টে/দলিলে ডিজিটাল স্বাক্ষর প্রয়োগ

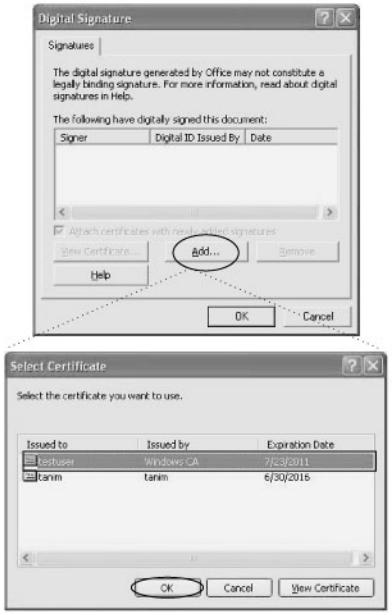
এ পর্যায়ে Microsoft office XP ব্যবহার করে কিভাবে একটি Word Document এ ডিজিটাল স্বাক্ষর প্রয়োগ করতে হয় তা দেখানো হবে। প্রথমে MS Word XP চালু করুন। কিছু বাক্য লিখুন। Document টি আপনার পছন্দ মত নাম দিয়ে সংরক্ষণ করুন এবং ডিজিটাল স্বাক্ষর প্রয়োগের জন্য চিত্র-১৬ এর ন্যায় নিচের পদক্ষেপ অনুসরণ করুন।

Tools মেনুতে ক্লিক করুন। মেনু থেকে 'Options' এ ক্লিক করুন। একটি ডায়ালগ বক্স খুলবে যেখানে অনেকগুলো ট্যাব দেখা যাবে। সেগুলির মধ্যে Security ট্যাবটিতে ক্লিক করুন। Security ট্যাব পেইজটিতে মাঝামাঝি জায়গায় Digital Signature নামে একটি বাটন দেখা যাবে। বাটনটিতে ক্লিক করুন।



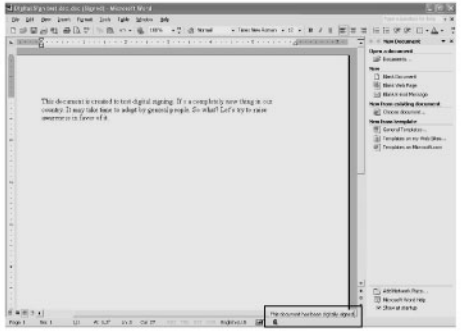
চিত্র-১৬

অতঃপর আপনাকে available signature to sign নামে একটি dialogue বক্স (চিত্র-১৭) দেখাবে। আপনার সার্টিফিকেট নির্বাচন করার জন্য add বাটনে ক্লিক করুন ও সার্টিফিকেট নির্বাচন করুন (চিত্র-১৭)। তাঁরপর Ok বাটন চাপুন।



চিত্র-১৭

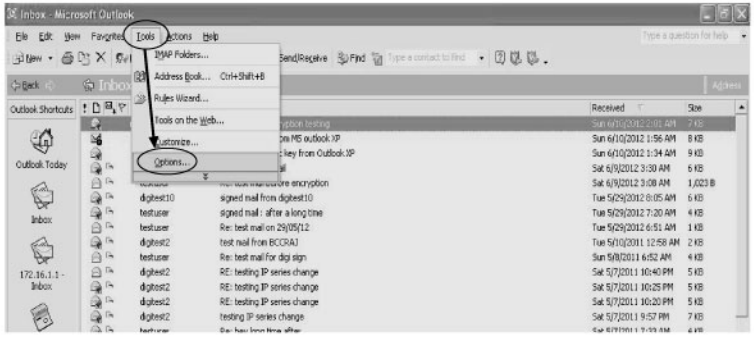
আপনার ডকুমেন্ট digitally স্বাক্ষরিত হয়ে গেল। আপনার document এর নিচের দিকে লাল ফিতা (Red Ribbon) সম্বলিত একটি চিহ্ন দেখাবে; তার উপর মাউস কার্সর ধরলে "the document is digitally signed" বার্তা দেখাবে (চিত্র-১৮)। যা থেকে প্রতীয়মান হয় ডকুমেন্টটি ডিজিটাল স্বাক্ষর দ্বারা স্বাক্ষরিত। বিস্তারিত দেখার জন্য লাল রিবনটিতে ডবল ক্লিক করুন।



চিত্র-১৮

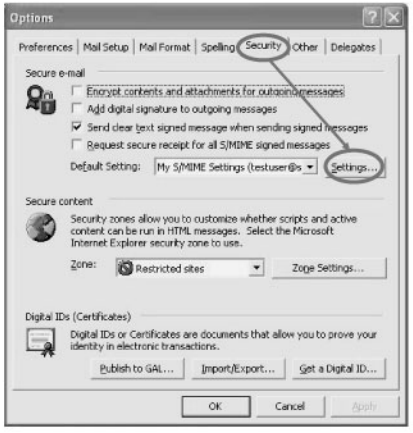
(ঘ) ডিজিটাল স্বাক্ষর সার্টিফিকেট ব্যবহার করে ইমেইল স্বাক্ষর

ই-মেইলে ডিজিটাল স্বাক্ষর প্রয়োগের জন্য যে কোন ই-মেইল ক্লায়েন্ট সফটওয়্যার ব্যবহার করতে পারেন। এ নির্দেশিকায় MS outlook mail client এ ডিজিটাল স্বাক্ষরের প্রয়োগ দেখানো হবে। প্রথমে আপনার Outlook মেইল ক্লায়েন্ট চালু করুন। সতর্কতা স্বরূপ দেখে নিন আপনার সার্টিফিকেটটি Outlook সফটওয়্যারে নির্বাচিত আছে কিনা। সেজন্য Tools মেনুতে ক্লিক করুন। মেনু থেকে 'Options' এ ক্লিক করুন (চিত্র-১৯)।



চিত্র-১৯

একটি নতুন ডায়ালগ বক্স খুলবে (চিত্র-২০)। সেখানে অনেকগুলো ট্যাব দেখা যাবে; তন্মধ্যে Security ট্যাবটিতে ক্লিক করুন।

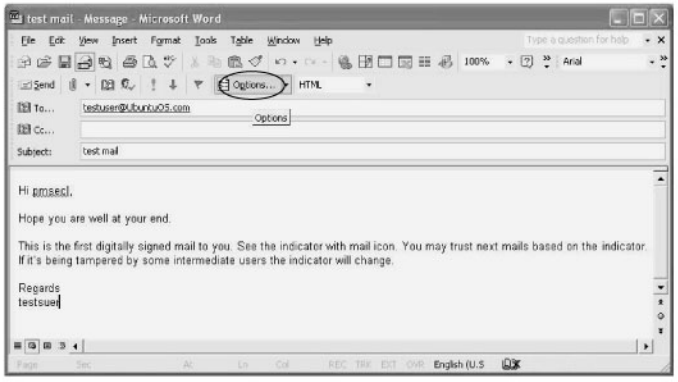


চিত্র-২০

যে পেইজটি দেখা যাবে, সেখানে "Default Settings" টেক্সট বক্সটি পরীক্ষা করে দেখুন যে সার্টিফিকেটটি ব্যবহারকারীর কিনা। "Settings" এ ক্লিক করলে সে "Signature Details" দেখাবে (চিত্র-২১)। আপনার যদি একাধিক সার্টিফিকেট থাকে, তাহলে গোলাকার চিহ্নিত 'Choose' বাটনে ক্লিক করে পরিবর্তন করে নিতে পারেন।

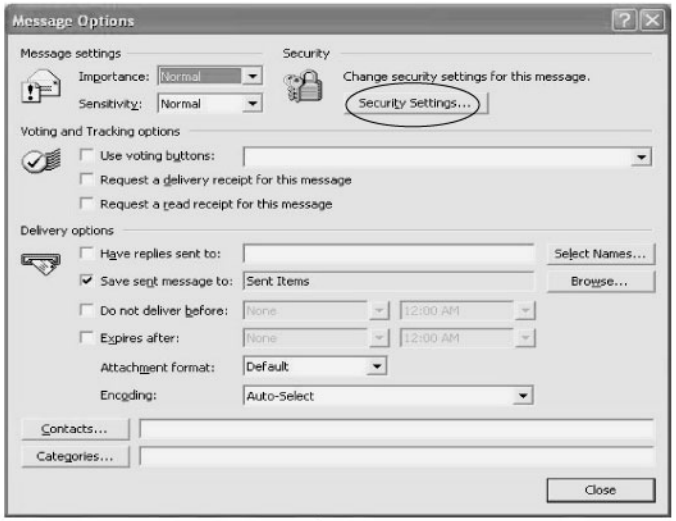
চিত্র-২১

এখন নতুন একটি মেইল লিখুন। লেখা হয়ে গেলে, ডিজিটাল স্বাক্ষর সংযুক্ত করার জন্য মেইল এডিটর (Mail editor) এর টুলবার থেকে Options লেখাটির উপর ক্লিক করুন (চিত্র-২২)। ফলে "Message options" ডায়ালগ বক্স (চিত্র-২৩) দেখাবে।



চিত্র-২২

ডায়ালগ বক্সটিতে গোলাকার চিহ্নিত "Security Settings" বাটনে ক্লিক করুন (চিত্র-২৩)।



চিত্র-২৩

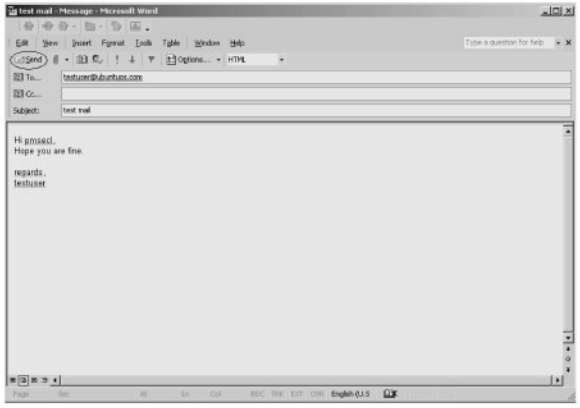
বাটনে ক্লিক করা হলে "Security Properties" ডায়ালগ বক্স (চিত্র-২৪) দেখাবে। ডায়ালগ বক্সটিতে "Add digital signature to this message" এর বাম পাশের Selection বক্সটিতে ক্লিক করুন। একটি টিক চিহ্ন দেখাবে। "Security Settings" টেক্সট বক্সটিতে আপনার সার্টিফিকেট নির্বাচন করুন।

চিত্র-২৪

পরবর্তীতে (চিত্র-২৫) গোলাকার চিহ্নিত ok বাটনে ক্লিক করুন। আপনার মেইলটি ডিজিটাল স্বাক্ষর দ্বারা স্বাক্ষরিত হয়ে গেল।

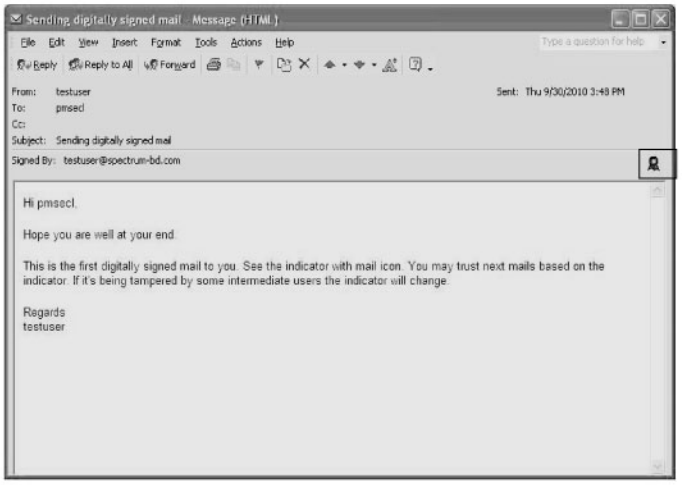
চিত্র-২৫

চিত্র-২৬ এ গোলাকার চিহ্নিত send বাটনে ক্লিক করুন। আপনার মেইলটি সফলভাবে digitally স্বাক্ষরিত হয়ে পাঠানো হয়েছে।



চিত্র-২৬

প্রেরণকৃত মেইলটি দেখার জন্য আপনার mail box এ sent ফোল্ডারে যান। যে মেইলটি একটু আগে পাঠিয়েছেন সেটি খুলুন। মেইলটির বাম পাশে গোলাকার সম্বলিত চিহ্ন দেখাবে অর্থাৎ আপনার মেইলটিতে ডিজিটাল স্বাক্ষর যুক্ত হয়েছে। চিত্র-২৭ এ চিহ্নিত লাল ফিতার উপর উপর ক্লিক করলে একটি ডায়ালগ পেইজ খুলবে।



চিত্র-২৭

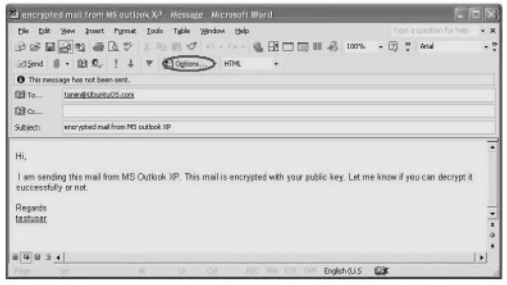
ডায়ালগ বক্সটিতে (চিত্র-২৮) আপনার স্বাক্ষর এবং এর বৈধতা সংক্রান্ত তথ্যাদি প্রদর্শন করবে। প্রাপকও তার Inbox ফোল্ডারে যখন প্রাপ্ত মেইলটি খুলবেন, একই চিহ্ন সম্বলিত অবস্থায় দেখতে পাবেন। চিহ্নটির উপর ক্লিক করলে প্রেরকের ডিজিটাল স্বাক্ষর এবং এর বৈধতা সংক্রান্ত তথ্যাদি প্রদর্শন করবে।

চিত্র-২৮

(৬) ইমেইল এনক্রিপশন

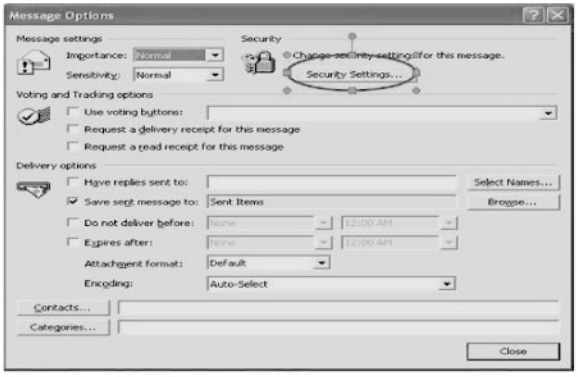
শুরু করার আগে যাচাই করে নিন আপনার Outlook Address Book এ প্রাপকের ডিজিটাল সার্টিফিকেট আছে কিনা। অন্যথায়, মেইল পাঠানোর সময় ভুলবার্তা দেখাবে এবং আপনি কখনোই এনক্রিপ্টেড মেইল পাঠাতে সক্ষম হবেন না। আপনি প্রাপকের ডিজিটাল সার্টিফিকেট সিএ'র LDAP সার্ভার থেকে অথবা প্রাপকের নিকট থেকে পূর্বে প্রেরিত ডিজিটাল স্বাক্ষর সার্টিফিকেট দ্বারা স্বাক্ষরিত মেইল থেকে সংগ্রহ করতে পারেন। আপনি Outlook দিয়ে স্বয়ংক্রিয় ভাবে সব মেইল অথবা শুধু নির্দিষ্ট মেইলগুলি এনক্রিপটেড করে পাঠানোর জন্য ব্যবস্থা করতে পারেন।

এনক্রিপশন করে নতুন মেইল পাঠানোর জন্য Outlook চালু করুন। এতে প্রথমে প্রাপক এর ঠিকানা সঠিক ভাবে লিখুন, মেইলের বিষয় এবং মূল কথা/বাক্য গুলি লিখুন। অতঃপর (চিত্র-২৯) চিহ্নিত 'Options' এ ক্লিক করুন।



চিত্র-২৯

'Options' এ ক্লিক করলে Message Options ডায়ালগ বক্স (চিত্র-৩০) খুলবে।

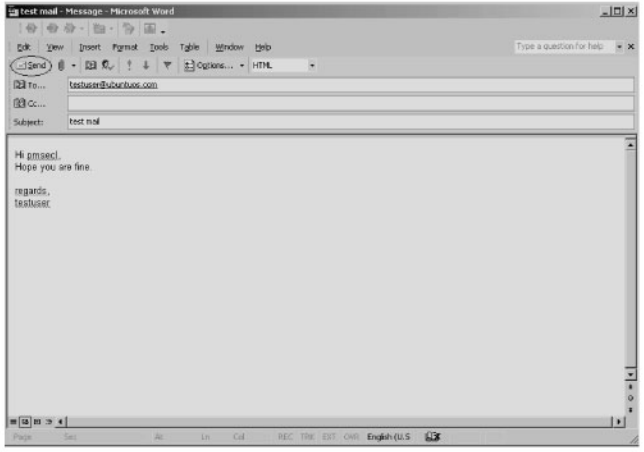


চিত্র-৩০

ডায়ালগ বক্সটিতে উপরের দিকে চিহ্নিত 'Security Settings' বাটন দেখতে পাবেন। বাটনটিতে ক্লিক করলে Security Properties নামে ডায়ালগ বক্স (চিত্র-৩১) প্রদর্শিত হবে।

চিত্র-৩১

বক্সটিতে 'Encrypt message contents and attachments' নামে চেক বক্সে টিক চিহ্ন দিন এবং চিহ্নিত 'Ok' বাটনে ক্লিক করুন। এখন আপনি এনক্রিপশন করে মেইল পাঠাতে প্রস্তুত হয়ে গেলেন।



চিত্র-৩২

চিত্র-৩২ এ গোলাকার চিহ্নিত 'Send' বাটনে ক্লিক করে মেইলটি পাঠিয়ে দিন। 'Sent' ফোল্ডারে ক্লিক করলে আপনি দেখতে পাবেন পাঠানো মেইলটি এনক্রিপশন অবস্থায় প্রেরিত হয়েছে। এটি বুঝার জন্য ডান পাশে একটি তালার আইকন দেখতে পাবেন (চিত্র-৩৩)।

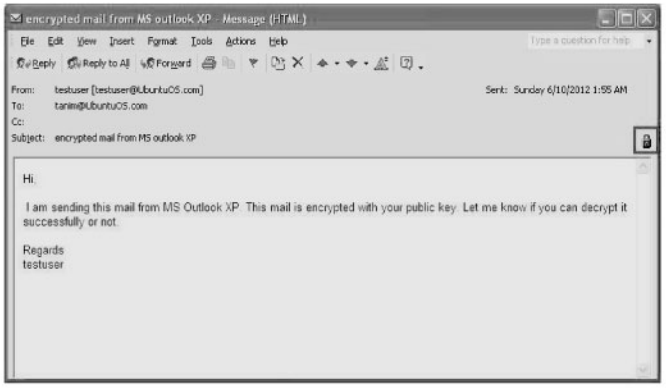
চিত্র-৩৩

এখন তালার আইকনটিতে ক্লিক করলে একটি মেসেজ বক্স খুলবে (চিত্র-৩৪)। যেখানে মেসেজটির এনক্রিপশন সংক্রান্ত তথ্য দেখতে পারবেন।

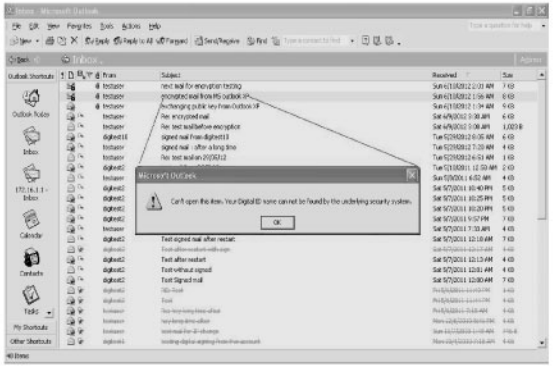
চিত্র-৩৪

প্রাপক যখন 'Inbox' থেকে মেইল খুলবেন তিনিও এনক্রিপশন 'symbol' দেখতে পাবেন (চিত্র-৩৫)। এনক্রিপশন 'symbol' এ ক্লিক করলে এনক্রিপশন সংক্রান্ত বিস্তারিত দেখতে পাবেন।

প্রাপকের কাছে তার নিজের প্রাইভেট কী সংযুক্ত সার্টিফিকেট না থাকলে প্রাপক এনক্রিপ্টেড মেসেজ পড়তে পারবে না এবং সেক্ষেত্রে একটি ভুলবার্তা দেখাবে (চিত্র-৩৬) কারণ আপনার Outlook মেসেজটি ডিক্রিপ্ট করতে অক্ষম। Outlook মেসেজটি ডিক্রিপ্ট করার জন্য প্রাপকের প্রাইভেট কী ব্যবহার করে থাকে।



চিত্র-৩৫



চিত্র-৩৬

৪.১.২. লিনাক্স অপারেটিং সিস্টেমে ডিজিটাল স্বাক্ষর ব্যবহার

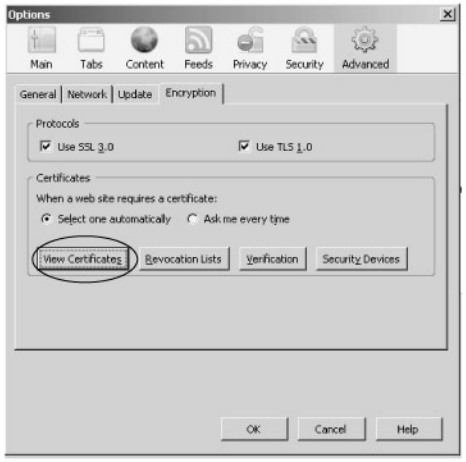
এ নির্দেশিকায় লিনাক্স অপারেটিং সিস্টেমে ডিজিটাল স্বাক্ষরের প্রয়োগ দেখানোর জন্য উবুন্টু অপারেটিং সিস্টেম ব্যবহার করা হয়েছে। উইন্ডোজ অপারেটিং সিস্টেমের ন্যায় এক্ষেত্রেও ডিজিটাল স্বাক্ষর সার্টিফিকেট ডিফল্ট ব্রাউজারে ইনস্টল করতে হবে। উবুন্টু অপারেটিং সিস্টেমে ডিফল্ট ব্রাউজার হলো মজিলা ফায়ারফক্স।

(ক) মজিলা ব্রাউজারে ব্যক্তিগত সার্টিফিকেট import করার পদ্ধতি

প্রথমে মজিলা ফায়ারফক্স চালু করুন। ডেস্কটপ এর উপরের টুলবারে মজিলার আইকনে ক্লিক করে অথবা Applications→ Internet→FireFox Web Browser মেনু থেকেও মজিলা চালু করা যেতে পারে।

চিত্র-৩৭

ফায়ারফক্স চালু করার পর চিত্র-৩৭ এ চিহ্নিত Edit মেনুতে ক্লিক করুন এবং তারপর নিচে চিহ্নিত preferences সাবমেনুতে ক্লিক করলে একটি বক্স চালু হবে (চিত্র-৩৮)।



চিত্র-৩৮

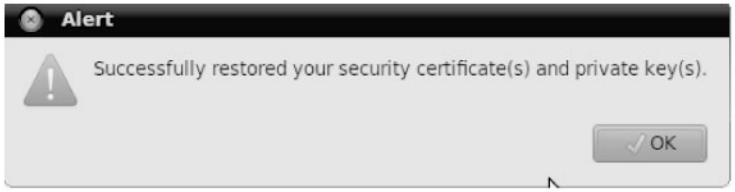
বক্সটির উপরে 'Advanced' ট্যাবে ক্লিক করলে 'Encryption' নামে একটি ট্যাব দেখতে পাবেন। 'Encryption' ট্যাবটিতে ক্লিক করলে 'View certificates' নামে একটি বাটন দেখতে পাবেন। 'View certificates' এ ক্লিক করলে 'Certificate Manager' নামে একটি ডায়ালগ বক্স (চিত্র-৩৯) চালু হবে।

চিত্র-৩৯

বক্সটির উপরের অংশের বাম পাশে গোলাকার চিহ্নিত 'Your certificates' লিংকটিতে ক্লিক করলে বিদ্যমান সার্টিফিকেটগুলির তালিকা প্রদর্শিত হবে। নিচে গোলাকার চিহ্নিত 'Import' বাটন দেখতে পাবেন যেখানে ক্লিক করলে একটি নতুন ডায়ালগ বক্স খুলবে। ব্যক্তিগত সার্টিফিকেটটি যেখানে রাখা আছে, ব্রাউজ করে সেখানে যেতে হবে। এখন আপনার ব্যক্তিগত সার্টিফিকেট ফাইলটি অর্থাৎ pkcs12 ফাইল নির্বাচন করুন। Import এর জন্য পাসওয়ার্ড লিখুন (চিত্র-৪০)।

পাসওয়ার্ড যদি ঠিকমত হয় তাহলে আপনি একটি সফলবার্তা (চিত্র-৪১) দেখতে পাবেন। অন্যথায় আপনাকে পুনরায় ঠিকমত পাসওয়ার্ড দিতে হবে।

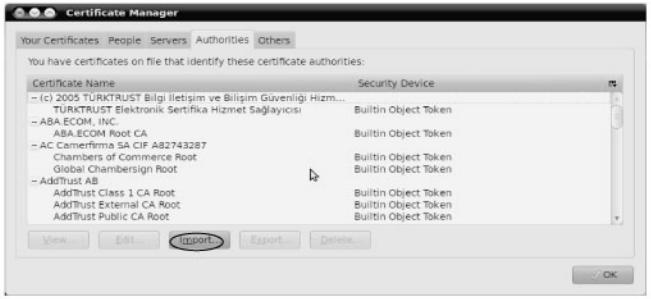
চিত্র-৪০



চিত্র-৪১

(খ) মজিলা ব্রাউজারে সিএ সার্টিফিকেট 'Import' করার পদ্ধতি

এবার একই নিয়মে সিএ সার্টিফিকেটটি মজিলাতে Import করে ফেলতে হবে। ধরে নেওয়া যাক আপনি Certificate Manager ডায়ালগ বক্সটিতে রয়েছেন। Authorities ট্যাবটিতে ক্লিক করুন (চিত্র-৪২)। যে সকল সিএ/ রুটসিএ (Root CA) এর সার্টিফিকেট মজিলাতে Import করা আছে সেগুলোর তালিকা দেখা যাবে।

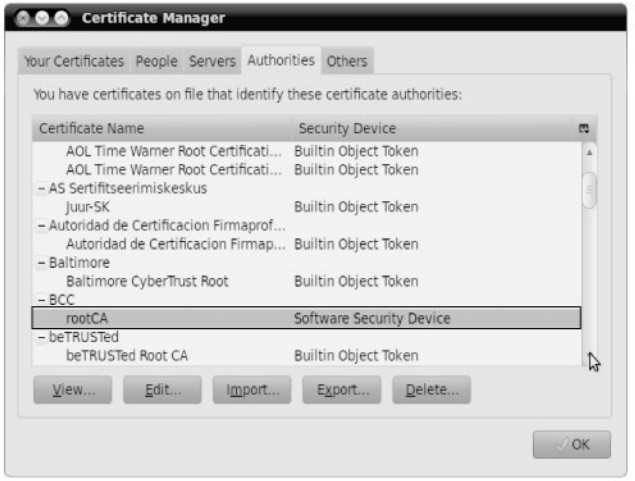


চিত্র-৪২

চিত্র-৪২ এ গোলাকার চিহ্নিত Import বাটনটিতে ক্লিক করুন এবং ব্যক্তিগত সার্টিফিকেটের মত ধাপগুলো অনুসরণ করুন। শেষ পর্যায়ে একটি সতর্কবার্তা (চিত্র-৪৩) দেখাবে। গোল চিহ্নিত দুইটি চেক বক্সে ক্লিক করে Ok বাটনে ক্লিক করুন।

চিত্র-৪৩

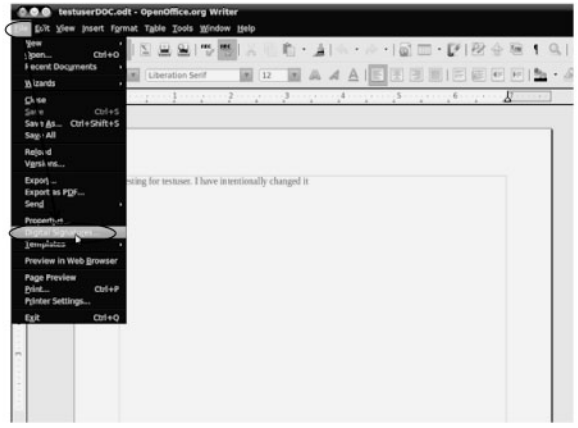
আপনার সিএ সার্টিফিকেটটি সফলভাবে import হবে এবং তালিকায় সার্টিফিকেটটি দেখা যাবে (চিত্র-৪৪)।



চিত্র-৪৪

(গ) ডকুমেন্টে/দলিলে স্বাক্ষর প্রয়োগ

উবুন্টু অপারেটিং সিস্টেমে Open Office নির্ধারিত (default) ডকুমেন্ট এডিটর হিসাবে কাজ করে। Open Office চালু করার জন্য Applications → Office → Open Office.org Word Processor লিংকে ক্লিক করুন। এখন ডিজিটাল স্বাক্ষর যুক্ত করার জন্য Open Office এ একটি নতুন ডকুমেন্ট ফাইল ওপেন করুন এবং তাতে লিখুন, অতঃপর একটি উপযুক্ত নাম দিয়ে সংরক্ষণ (save) করুন।

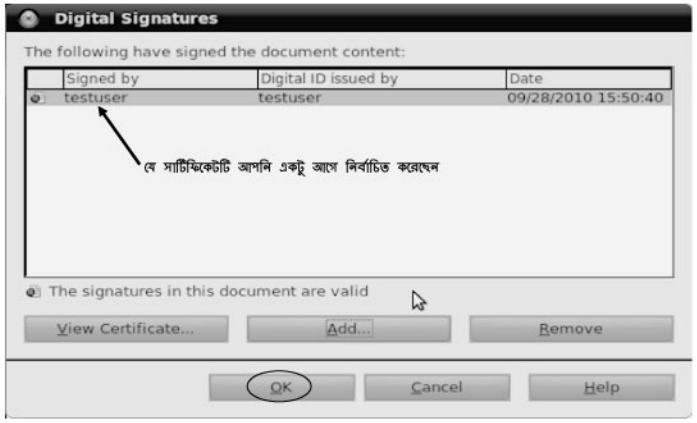


চিত্র-৪৫

ফাইলটি সংরক্ষণ করার পর চিত্র-৪৫ এ চিহ্নিত File মেনুতে ক্লিক করে গোলাকার চিহ্নিত 'Digital Signatures' সাবমেনুতে ক্লিক করলে একটি ডায়াগল বক্স (চিত্র-৪৬) খুলবে।

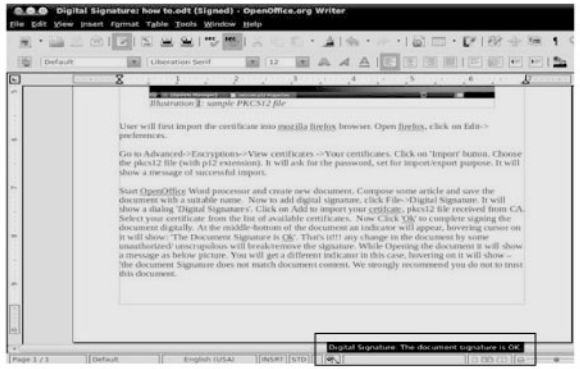
চিত্র-৪৬

ডায়ালগ বক্সটিতে গোলাকার চিহ্নিত 'Add' বাটনে ক্লিক করলে নতুন আরেকটি ডায়ালগ বক্স (চিত্র-৪৭) খুলবে।



চিত্র-৪৭

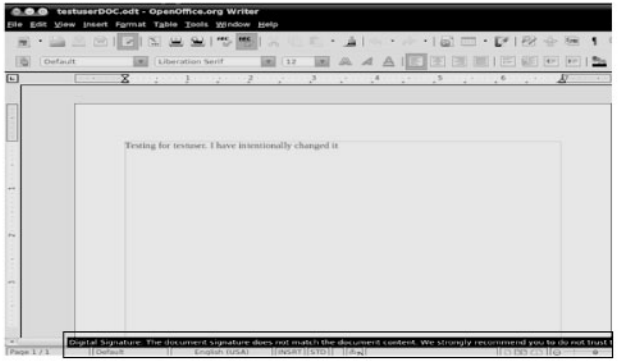
বক্সটিতে সার্টিফিকেটের তালিকা দেখতে পাবেন। তালিকা থেকে আপনার সার্টিফিকেটটি নির্বাচন করুন এবং চিত্র-৪৭ এ গোলাকার চিহ্নিত 'ok' বাটনে ক্লিক করুন। আপনার ডকুমেন্টটি নির্বাচিত সার্টিফিকেট দ্বারা স্বাক্ষরিত হয়ে গেল।



চিত্র-৪৮

চিত্র-৪৯

ডকুমেন্টটির নিচের অংশে একটি আইকন দেখতে পাবেন (চিত্র-৪৮)। এতে মাউস কার্সর রাখলে 'The Document Signature is Ok' বার্তা দেখতে পাবেন। স্বাক্ষর করা ডকুমেন্টে যদি অন্য কেউ কোন পরিবর্তন করেন তবে উক্ত ডকুমেন্ট খুললে একটি অবহিতকরণ বার্তা (চিত্র-৪৯) দেখাবে। এ থেকে আপনি নিশ্চিত হতে পারেন যে, স্বাক্ষরিত ডকুমেন্টটি আপনার অগোচরে কেউ পরিবর্তন করেছে।

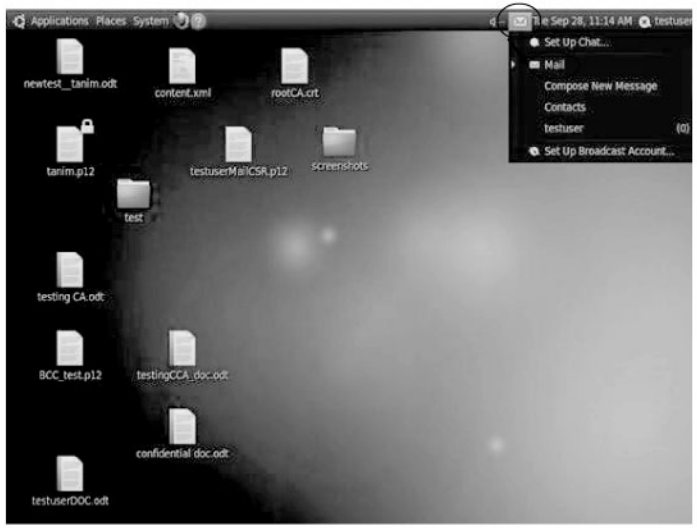


চিত্র-৫০

এছাড়াও আপনি ডকুমেন্টের নিচের অংশে একটি আইকন দেখতে পাবেন যাতে মাউস কার্সর রাখলে 'the document signature does not match document content. We strongly recommend you do not trust this document.' লেখা দেখতে পাবেন (চিত্র-৫০)।

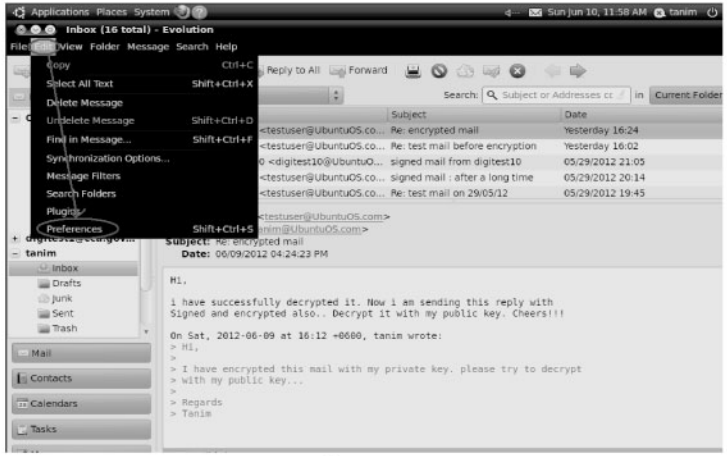
(ঘ) ইমেইলে ডিজিটাল স্বাক্ষর

উবুন্টু (Ubuntu) ১০.০৪ এ নির্ধারিত (default) মেইল ক্লায়েন্ট হিসাবে Evolution ইনস্টল করা থাকে। উবুন্টু ডেস্কটপ এর Evolution মেইল ক্লায়েন্ট থেকে উপরের ডান কর্ণারের চিহ্নিত আইকনে (চিত্র-৫১) ক্লিক করলে 'Mail' নামে লিংকটি দেখতে পাবেন। এর উপর ক্লিক করুন, তাহলে Evolution মেইল ক্লায়েন্ট সফটওয়্যারটি খুলবে।



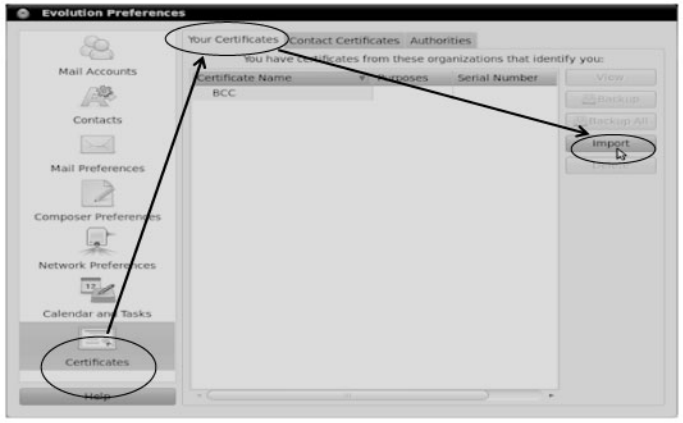
চিত্র-৫১

মেইলে ডিজিটাল স্বাক্ষরের জন্য প্রথমে pkcs12 ফাইল import করা প্রয়োজন। Evolution সফটওয়্যারের Edit মেনুতে ক্লিক করলে নিচে Preferences নামে সাবমেনু দেখতে পাবেন (চিত্র-৫২)।



চিত্র-৫২

Preferences সাবমেনুতে ক্লিক করলে একটি ডায়ালগ বক্স (চিত্র-৫৩) খুলবে। বক্সটির নিচের দিকে certificates নামে চিহ্নিত আইকন দেখতে পাবেন। আইকনটিতে ক্লিক করলে Your Certificates ট্যাব দেখতে পাবেন। Your Certificates ট্যাবটিতে ক্লিক করলে বিদ্যমান সার্টিফিকেট গুলোর একটি তালিকা প্রদর্শন হবে। এখন ডান দিকে গোলাকার চিহ্নিত 'import' বাটনটিতে ক্লিক করুন।

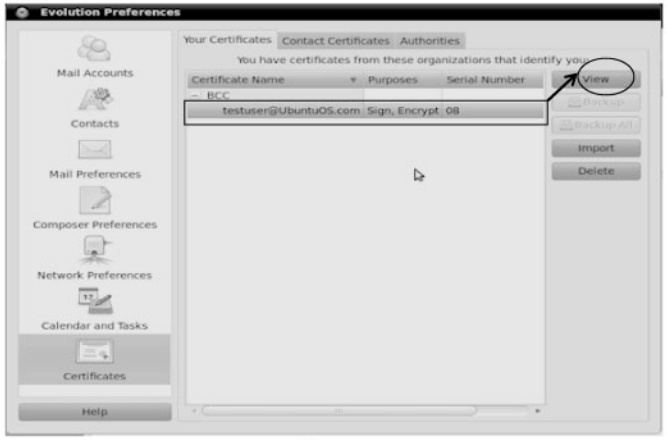


চিত্র-৫৩

অতঃপর একটি ফাইল ব্রাউজার খুলবে, সেখানে আপনার ব্যক্তিগত pkcs12 ফাইলটি Ubuntu ফাইল সিস্টেম থেকে নির্বাচন করুন। এর জন্য আপনাকে ২টি পাসওয়ার্ড দিতে হবে (চিত্র-৫৪)। একটি Evolution মেইল ক্লায়েন্ট এর নিরাপত্তার জন্য এবং অন্যটি import/export এর জন্য।

চিত্র-৫৪

সঠিকভাবে পাসওয়ার্ড দেওয়া হলে Evolution মেইল ক্লায়েন্ট এ সার্টিফিকেট সফলভাবে import হবে এবং তালিকায় imported সার্টিফিকেটটি দেখা যাবে (চিত্র-৫৫)।



চিত্র-৫৫

চিত্র-৫৫ এ গোলাকার চিহ্নিত 'view' বাটনে ক্লিক করলে সার্টিফিকেট এর বিস্তারিত দেখতে পাবেন (চিত্র-৫৬)।

চিত্র-৫৬

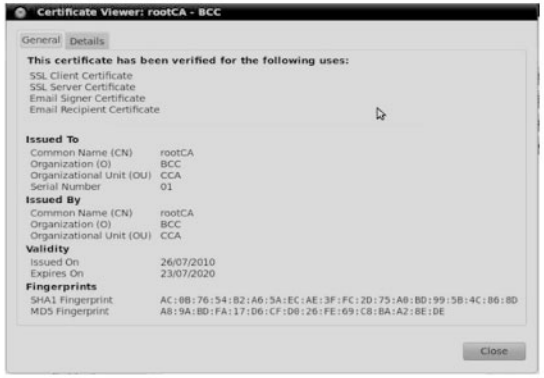
উপরের মত একইভাবে Evolution সফটওয়্যারে Edit মেনুতে ক্লিক করলে 'Preferences' নামে সাবমেনু দেখতে পাবেন তাতে ক্লিক করলে 'Certificates' নামে চিহ্নিত আইকন দেখতে পাবেন। 'Certificates' আইকনে ক্লিক করলে 'Authorities' ট্যাব দেখতে পাবেন। ট্যাবটিতে ক্লিক করলে সেখানে বিদ্যমান সিএ/রুট (Root) সিএ সার্টিফিকেটের একটি তালিকা প্রদর্শিত হবে। এখন ডান দিকে Import নামে একটি বাটন দেখা যাবে (চিত্র-৫৭)।

চিত্র-৫৭

চিত্র-৫৭ এ গোলাকার চিহ্নিত Import বাটনে ক্লিক করলে একটি ফাইল ব্রাউজার খুলবে, সেখান থেকে CA সার্টিফিকেট ফাইলটি নির্বাচন করলে একটি ডায়ালগ বক্স (চিত্র-৫৮) খুলবে।

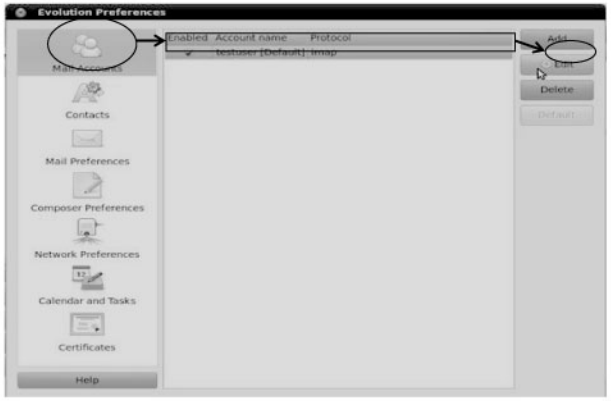
চিত্র-৫৮

ডায়ালগ বক্সটিতে 'Trust this CA to identify web sites' এবং 'Trust this CA to identify email users' চেক বক্সে টিক চিহ্ন দিন তারপর 'OK' বাটনে ক্লিক করুন। সিএ সার্টিফিকেটটি সফলভাবে Evolution সফটওয়্যারে import হবে। সিএ/রুট (Root) সিএ সার্টিফিকেটের তালিকা থেকে আপনি কেবল যে সার্টিফিকেটটি import করেছেন সেটি নির্বাচন করুন। বক্সটির ডান দিকে 'View Certficate' বাটনে ক্লিক করলে CA সার্টিফিকেটের বিস্তারিত (চিত্র-৫৯) দেখতে পাবেন।



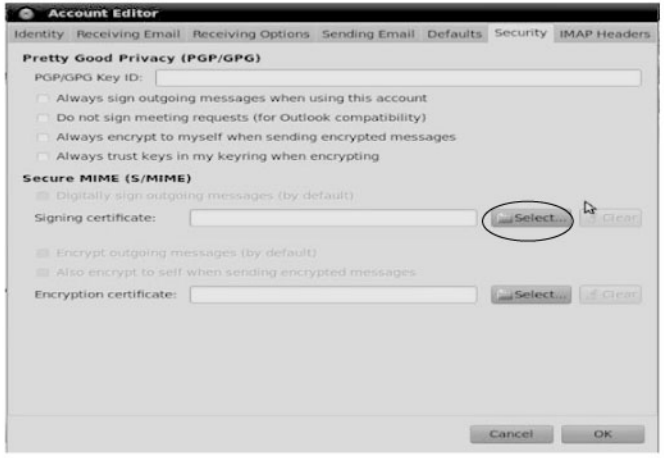
চিত্র-৫৯

এখন আপনার নামে Evolution এর মধ্যে যে অ্যাকাউন্ট রয়েছে, সেখানে আপনার ব্যক্তিগত সার্টিফিকেটটি দেখিয়ে দিতে হবে। সুতরাং উপরের মত একইভাবে Evolution এর Edit মেনুতে ক্লিক করে Preferences সাবমেনুতে ক্লিক করলে একটি ডায়ালগ বক্স খুলবে। বক্সটির বাম পাশে উপরের দিকে গোলাকার চিহ্নিত (চিত্র-৬০) 'Mail Accounts' লিংকটি দেখতে পাবেন তাতে ক্লিক করলে ব্যবহারকারীর একাউন্টের বিস্তারিত দেখতে পাবেন।



চিত্র-৬০

এখন আপনার একাউন্টটি নির্বাচিত করে ডান পার্শ্বে চিহ্নিত 'Edit' বাটনে ক্লিক করলে একটি ডায়ালগ বক্স (চিত্র-৬১) প্রদর্শিত হবে, যেখানে বেশ কিছু ট্যাব দেখা যাবে।

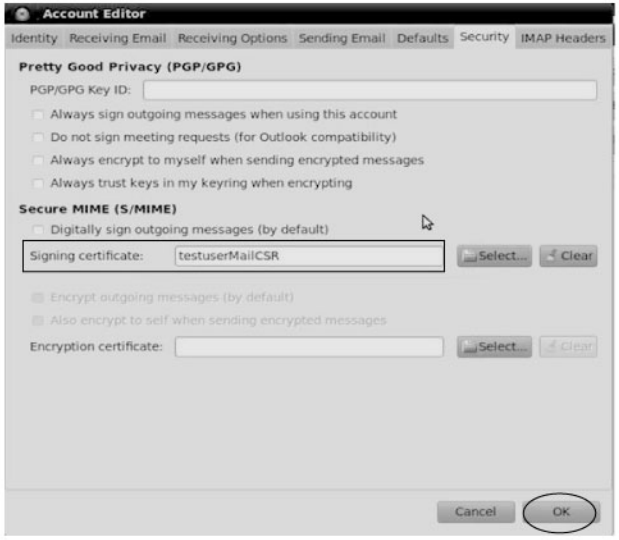


চিত্র-৬১

বক্সটির 'Security' ট্যাবে ক্লিক করলে আপনার অ্যাকাউন্টের সাথে সংযুক্ত সার্টিফিকেটের অবস্থা দেখা যাবে। যেহেতু আমরা এটি প্রথমবারের মত করছি, সুতরাং কোন সার্টিফিকেট দেখা যাবে না। চিত্র-৬১ তে গোলাকার চিহ্নিত 'select' বাটনে ক্লিক করে মেইল স্বাক্ষরের জন্য আপনার সার্টিফেকেট নির্বাচন করুন (চিত্র-৬২)।

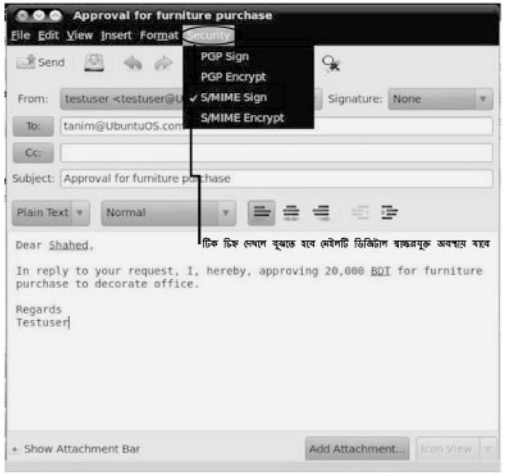
চিত্র-৬২

এখন 'ok' বাটনে ক্লিক করলে আপনার মেইল একাউন্ট ডিজিটাল স্বাক্ষর করে মেইল পাঠানোর জন্য উপযোগী হয়ে যাবে। চিত্র-৬৩ এ দেখা যাচ্ছে আপনার নির্বাচিত সার্টিফিকেটটি Signing certificate হিসাবে উল্লেখিত রয়েছে। ডায়ালগ পেইজটি বন্ধ করার জন্য Ok বাটন ক্লিক করুন।



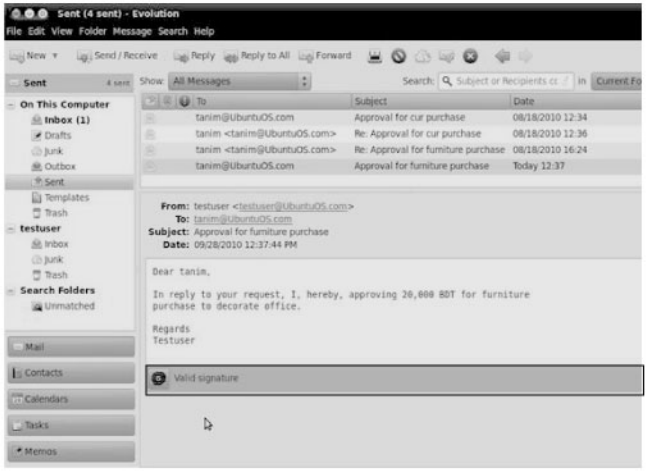
চিত্র-৬৩

এখন একটি নতুন মেইল লিখুন। পাঠানোর আগে আপনাকে বলে দিতে হবে এটি ডিজিটাল স্বাক্ষরযুক্ত হবে কিনা। সেজন্য চিত্র-৬৪ এ গোলাকার চিহ্নিত 'Security' মেনুতে ক্লিক করলে নিচে 'S/MIME Sign' সাবমেনু দেখতে পাবেন। তাতে ক্লিক করলে মেনুটি নির্বাচিত বা টিক চিহ্ন অবস্থায় দেখতে পাবেন।



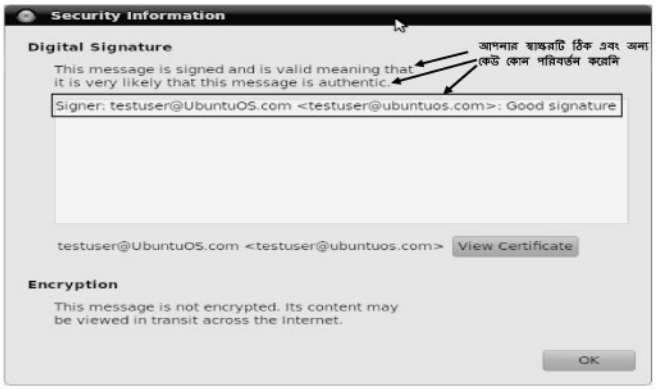
চিত্র-৬৪

এখন মেইলটি পাঠিয়ে দিন। মেইলটি ডিজিটাল স্বাক্ষরসহ প্রেরিত হল। আপনার Sent ফোল্ডারে গিয়ে যে মেইলটি পাঠিয়েছেন সেটি নির্বাচিত করুন (চিত্র-৬৫)। মেইলটির নিচের দিকে Valid Signature লেখাটি দেখতে পাবেন।



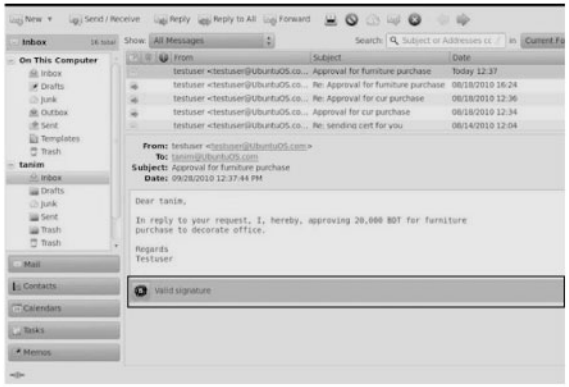
চিত্র-৬৫

Valid Signature লেখার বাম পার্শ্বে আইকনটির উপর ক্লিক করলে ডিজিটাল স্বাক্ষর সংক্রান্ত তথ্য প্রদর্শিত হবে (চিত্র-৬৬)।



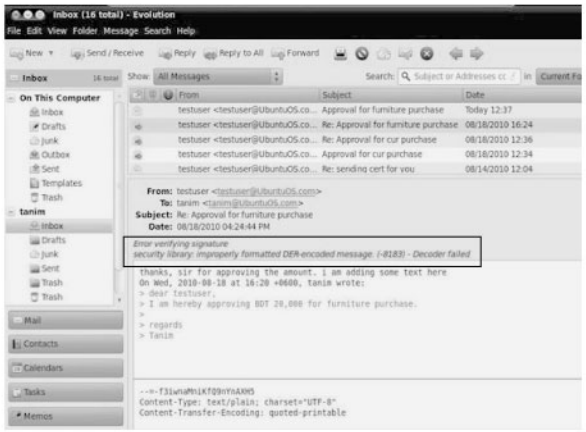
চিত্র-৬৬

প্রাপক যখন মেইল বক্স থেকে মেইল খুলবেন তখন একইভাবে Valid Signature লেখা দেখতে পাবেন। লেখাটির বাম পার্শ্বে আইকনের উপর ক্লিক করলে স্বাক্ষর সংক্রান্ত তথ্য প্রদর্শিত হবে (চিত্র-৬৭)।



চিত্র-৬৭

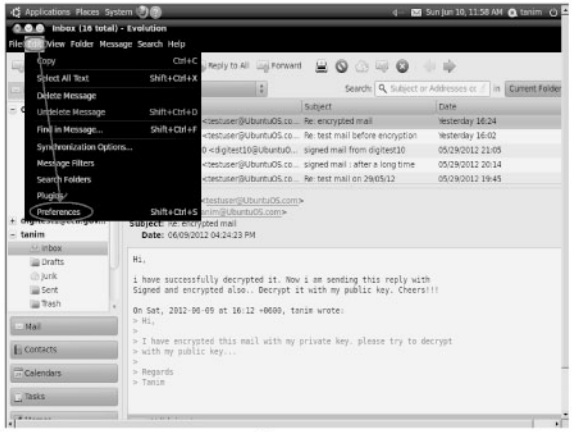
আর যদি অন্য কারও দ্বারা কোন পরিবর্তন সাধিত হয় তবে ওয়ার্নিং প্রদর্শন করবে (চিত্র-৬৮)। এ থেকে আপনি নিশ্চিত হতে পারবেন আপনার/প্রেরকের অগোচরে কেউ এটিতে পরিবর্তন করেছে।



চিত্র-৬৮

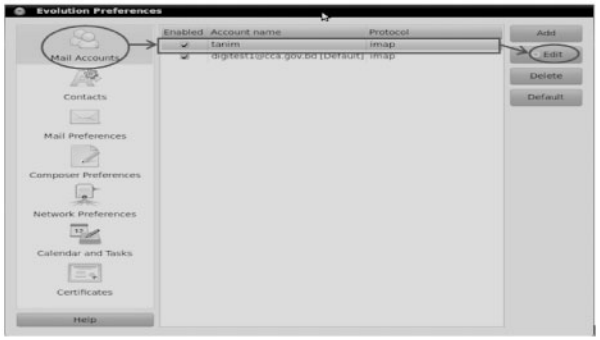
(ঙ) ইমেইল এনক্রিপশন

মেইল এনক্রিপশন বলতে এখানে পাবলিক কী দ্বারা এনক্রিপশনকে বুঝানো হয়েছে। অর্থাৎ প্রাপকের পাবলিক কী দিয়ে আপনি মেইল এনক্রিপ্ট করে পাঠাবেন। ফলে প্রাপকই শুধুমাত্র উক্ত মেইলটি তার প্রাইভেট কী দিয়ে decrypt করতে পারবেন। ধরে নেওয়া যাক আপনার Evolution মেইল ক্লায়েন্টটি খোলা অবস্থায় আছে। মেইল এনক্রিপ্ট করতে চাইলে 'Edit' মেনুতে ক্লিক করে 'preferences' সাবমেনুতে ক্লিক করুন (চিত্র-৬৯)।



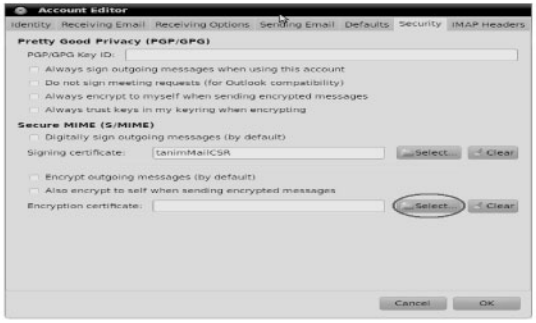
চিত্র-৬৯

অতঃপর একটি ডায়ালগ বক্স খুলবে। বক্সটিতে গোলাকার চিহ্নিত 'Mail Accounts' দেখতে পাবেন। 'Mail Accounts' এ ক্লিক করলে মেইল একাউন্টের তালিকা দেখতে পাবেন (চিত্র-৭০)।



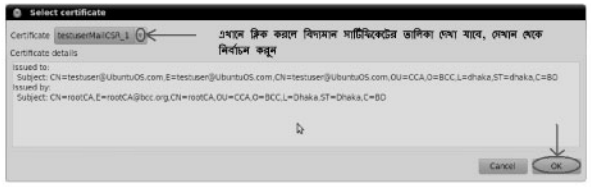
চিত্র-৭০

তালিকা থেকে আপনার একাউন্ট বাছাই করুন এবং ডান পাশে 'Edit' বাটনে ক্লিক করুন। ফলে একটি ডায়ালগ বক্স (চিত্র-৭১) খুলবে, যেখানে বেশকিছু ট্যাব দেখা যাবে। বক্সটিতে 'Security' নামে একটি ট্যাব দেখতে পাবেন। 'Security' ট্যাবে ক্লিক করুন। ক্লিক করার পর আপনার অ্যাকাউন্টের সাথে সংযুক্ত সার্টিফিকেটের নাম প্রদর্শিত হবে।



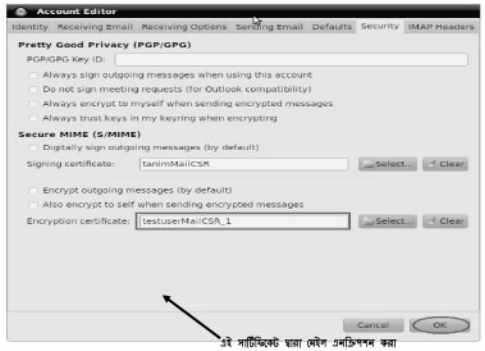
চিত্র-৭১

চিত্র-৭১ এ গোলাকার চিহ্নিত 'Select' বাটনে ক্লিক করুন যা আপনাকে এনক্রিপ্ট করার জন্য সার্টিফিকেট অনুসন্ধান করার ডায়লগ বক্সে নিয়ে যাবে। তালিকা থেকে আপনার সার্টিফিকেট নির্বাচন করুন (চিত্র-৭২) এবং 'OK' বাটনে ক্লিক করুন।



চিত্র-৭২

উপরোক্ত 'Ok' বাটনে ক্লিক করলে পূর্বের ডায়ালগ বক্সে ফেরত যাবেন এবং তাতে আপনার সার্টিফিকেট বাছাইকৃত অবস্থায় দেখতে পাবেন (চিত্র-৭৩)।

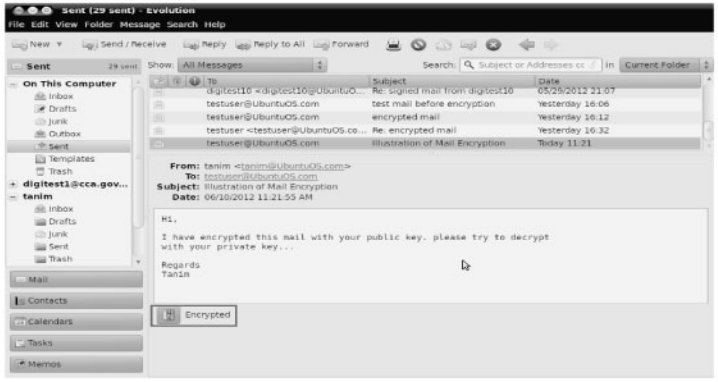


চিত্র-৭৩

চিত্র-৭৩ এ গোলাকার চিহ্নিত 'Ok' বাটনে ক্লিক করলে আপনার মেইল একাউন্টে এনক্রিপশন সার্টিফিকেট যুক্ত হয়ে গেল এবং এনক্রিপশন করে মেইল পাঠাতে পারবেন। এখন একটি নতুন মেইল প্রস্তুত করুন যা এনক্রিপ্ট করে পাঠাবেন। চিত্র-৭৪ এ গোলাকার চিহ্নিত 'Security' মেনুতে ক্লিক করলে নিচে 'S/MIME Encrypt' সাবমেনু দেখতে পাবেন তাতে ক্লিক করলে বাম পাশে টিক চিহ্ন অবস্থায় পাবেন।

চিত্র-৭৪

এখন 'Send' বাটনে ক্লিক করলে আপনার মেইল এনক্রিপটেড অবস্থায় প্রেরিত হবে। এখন আপনার মেইল বক্স থেকে 'Sent' ফোল্ডারে ক্লিক করুন। যে মেইলটি মাত্র পাঠিয়েছেন, সেটি বাছাই করুন। এখানে আপনি 'Encrypted' লেখা (চিত্র-৭৫) দেখতে পাবেন।

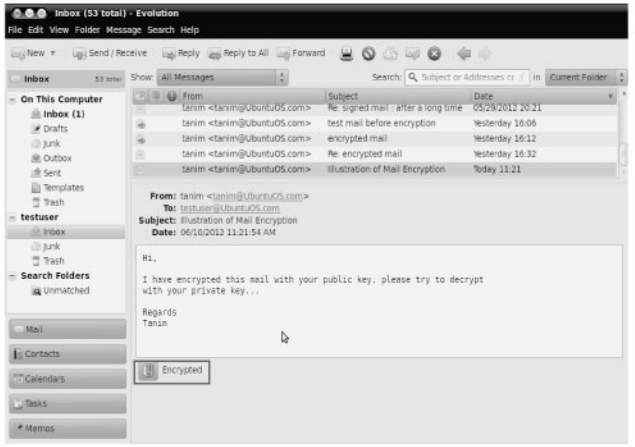


চিত্র-৭৫

এখন 'Encrypted' লেখার বাম পাশের আইকনে ক্লিক করলে মেইল এনক্রিপশনের বিস্তারিত তথ্য দেখতে পাবেন (চিত্র-৭৬)।

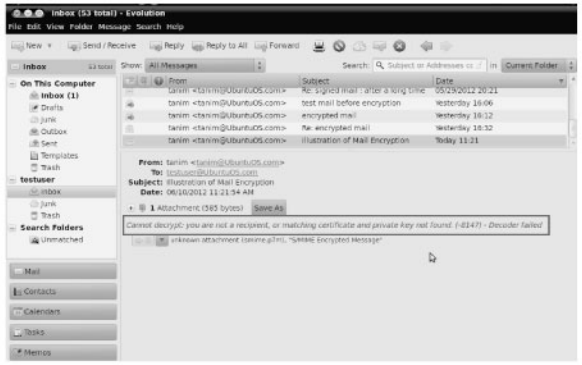
চিত্র-৭৬

প্রাপক যখন এনক্রিপটেড অবস্থায় মেইল পাবেন তখন Mail client ডিক্রিপ্ট করার জন্য প্রাপকের ব্যক্তিগত কী (private key) ব্যবহার করবে যাতে মেইলটি পড়া যায়। চিত্র-৭৭ এর মেইলটি পড়া যায় কারন এটি সফলভাবে ডিক্রিপ্ট করা গেছে।



চিত্র-৭৭

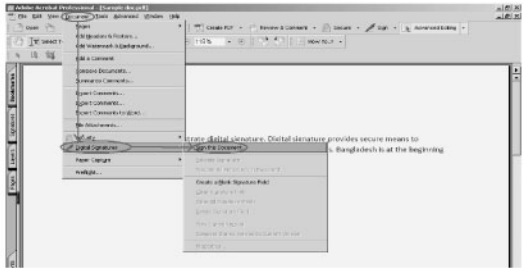
অন্যথায় প্রাপক এর কাছে যদি কোন ডিজিটাল সার্টিফিকেট না থাকে বা ডিজিটাল সার্টিফিকেট এর বৈধতা না থাকে তবে মেইলটির লেখা পড়তে পারবেনা, কারন তখন Mail client মেসেজটি ডিক্রিপ্ট করতে পারবে না (চিত্র-৭৮)। যা নিচের পেইজে চিহ্নিত মেসেজে বিদ্যমান।



চিত্র-৭৮

৪.১.৩ পিডিএফ ডকুমেন্টে ডিজিটাল স্বাক্ষর

ডিজিটাল স্বাক্ষর প্রয়োগ করে পিডিএফ ফাইলও স্বাক্ষর করতে পারবেন। এই জন্য আপনাকে Adobe Acrobat এর professional সংস্করণ ব্যবহার করে এই কাজটি করতে হবে। আপনি একটি পিডিএফ ফাইল খুলুন।

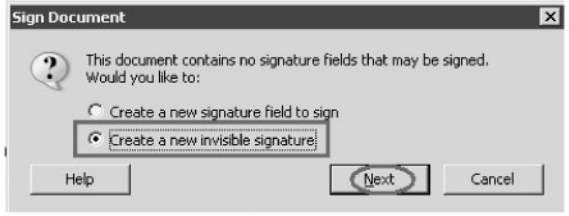


চিত্র-৭৯

ফাইলটি খোলার পর 'Document' মেনুতে ক্লিক করুন তারপর নিচে চিহ্নিত সাবমেনু 'Digital Signature' এ ক্লিক করলে ডান দিকে চিহ্নিত 'Sign this Document' সাবমেনু দেখতে পাবেন। 'Sign this Document' সাবমেনুতে ক্লিক করুন (চিত্র-৭৯)। ক্লিক করলে একটি মেসেজ বক্স খুলবে এবং তাতে লেখা থাকবে 'Document is not certified' (চিত্র-৮০)।

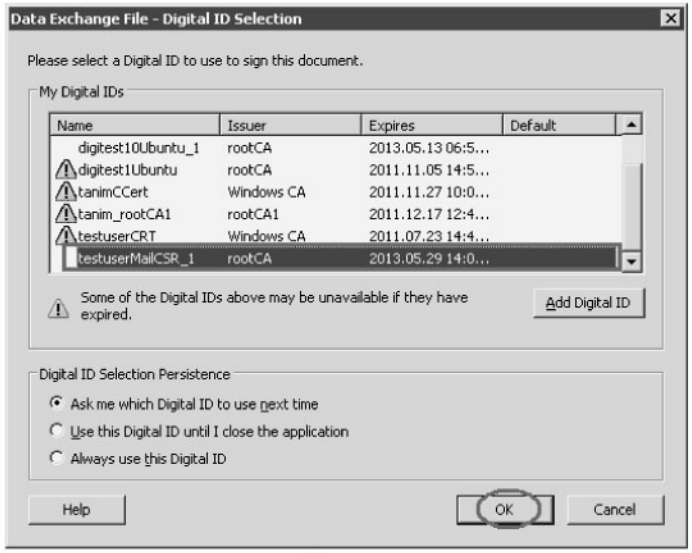
চিত্র-৮০

বক্সটির 'Coutinue Signing' বাটনে ক্লিক করলে আরেকটি মেসেজ বক্স (চিত্র-৮১) খুলবে, যেখানে আপনাকে ডকুমেন্টটিতে ডিজিটাল স্বাক্ষরের স্থান বিষয়ক একটি পদ্ধতি নির্বাচন করতে হবে।



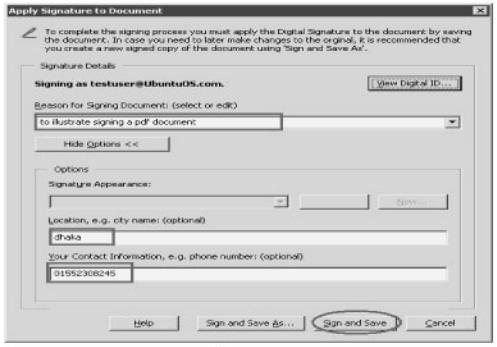
চিত্র-৮১

প্রথম রেডিও বাটনটিতে ক্লিক করে Next বাটনে ক্লিক করলে আপনি PDF ডকুমেন্টটির কোন স্থানে ডিজিটাল স্বাক্ষর প্রয়োগ করবেন তা নির্ধারন করতে পারবেন। অন্যদিকে দ্বিতীয় রেডিও বাটনটিতে ক্লিক করলে ডিজিটাল স্বাক্ষরটি ডকুমেন্টে অদৃশ্যমান থাকবে। এখন আপনি দ্বিতীয় রেডিও বাটনটি অর্থাৎ 'Create a new invisible signature' রেডিও বাটনে ক্লিক করে 'Next' বাটনে ক্লিক করুন। একটি ডায়ালগ বক্স (চিত্র-৮২) খুলবে, যেখানে অপারেটিং সিস্টেমের বিদ্যমান imported সার্টিফিকেটগুলি দেখা যাবে।



চিত্র-৮২

তালিকা থেকে আপনার সার্টিফিকেট নির্বাচন করুন এবং 'Ok' বাটনে ক্লিক করুন। নতুন একটি ডায়ালগ বক্স খুলবে, যেখানে ডিজিটাল স্বাক্ষর সংক্রান্ত কিছু মেটাডেটা থাকবে। এই বক্সটিতে স্বাক্ষরদাতা হিসাবে আপনার নাম দেখা যাবে (চিত্র-৮৩)।

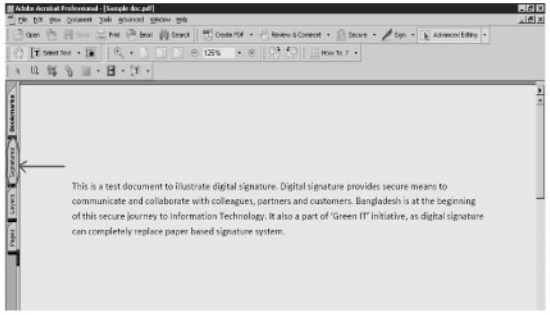


চিত্র-৮৩

বক্সটিতে চিহ্নিত 'Reason for Signing Document', 'Location' এবং 'Contact number' বক্সগুলোতে প্রয়োজনীয় তথ্য লিখতে পারেন এবং 'Sign & Save' বাটনে ক্লিক করুন। একটি সফলবার্তা (চিত্র-৮৪) দেখা যাবে।

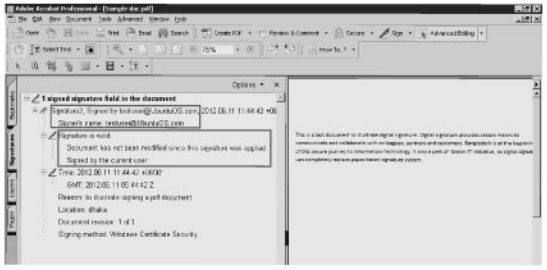
চিত্র-৮৪

'OK' বাটনে ক্লিক করুন। এখন পিডিএফ ফাইলে ডিজিটাল স্বাক্ষরের অবস্থা দেখতে চাইলে পিডিএফ ডকুমেন্টের বাম পাশে চিহ্নিত 'Signature' ট্যাবে (চিত্র-৮৫) ক্লিক করুন।



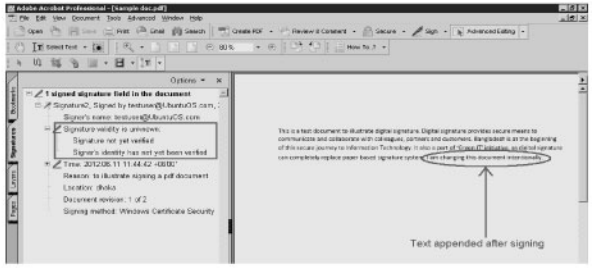
চিত্র-৮৫

Signature ট্যাবে ক্লিক করলে আপনি স্বাক্ষরদাতার নাম, স্বাক্ষর স্টেটাস, স্বাক্ষরের তারিখ/সময় দেখতে পাবেন। স্বাক্ষরের পর ডকুমেন্টে কোন রকম পরিবর্তন না হলে তাতে 'Signature is valid ' দেখতে পাবেন (চিত্র-৮৬)।



চিত্র-৮৬

যদি স্বাক্ষরকারী থেকে অনুমতি ছাড়া কেহ ডকুমেন্টে পরিবর্তন করে, তবে স্বাক্ষর অবস্থা পরিবর্তিত দেখতে পাবেন। যেমন স্বাক্ষরের পর ডকুমেন্টের কোন লেখা যোগ করলে বা বাদ দিলে 'Signature validity is unknown' লেখা দেখতে পাবেন (চিত্র-৮৭)।



চিত্র-৮৭

৪.২ ক্রিপটো (Crypto)/ হার্ড (Hard) টোকেন ব্যবহার পদ্ধতি

এই ডকুমেন্টের পূর্বের অংশে যে ব্যবহার পদ্ধতি বর্ণনা করা হয়েছে তা সফট টোকেন (অর্থাৎ ডিজিটাল সার্টিফিকেট ফাইল) দিয়ে ডিজিটাল স্বাক্ষর প্রয়োগ পদ্ধতি। ক্রিপটো বা হার্ড টোকেন দিয়েও ডিজিটাল স্বাক্ষর প্রয়োগ করা যায়, এটা সুবিধাজনকও বটে। টোকেনটি দেখতে ফ্ল্যাশ বা ইউএসবি (USB) ড্রাইভের মত, যা কম্পিউটার বা ল্যাপটপের USB পোর্টে সংযুক্ত করতে হয়।

ফ্ল্যাশ বা ইউএসবি ড্রাইভের মত দেখতে হলেও এটি আপনার কম্পিউটারে কোন ড্রাইভ হিসেবে দেখাবে না। এটির ভিতরের কনটেন্ট দেখতে হলে আপনাকে এর ড্রাইভার সফটওয়্যার ইনস্টল করতে হবে। ড্রাইভারটি ইনস্টল করা হলে আপনাকে আপনার টোকেনটি initialize করতে হবে। টোকেন initialize করার সময় আপনাকে pin/password দিতে হবে। এই pin/password টি হল টোকেনটির নিরাপত্তার জন্য।

অর্থাৎ টোকেনটি যদি কখনও হারিয়েও যায় কেউ এর কনটেন্ট ব্যবহার করতে পারবেনা। initialize এর সময় পরপর কয়েকবার ভুল হলে আপনার ক্রিপটো বা হার্ড টোকেনটি স্বয়ংক্রিয়ভাবে ব্যবহারের অনুপযুক্ত (disabled) হয়ে যাবে তা নির্ধারণ করে দেওয়া যায়। টোকেনটি সবসময় নিরাপদ কোন স্থানে সংরক্ষন করুন।

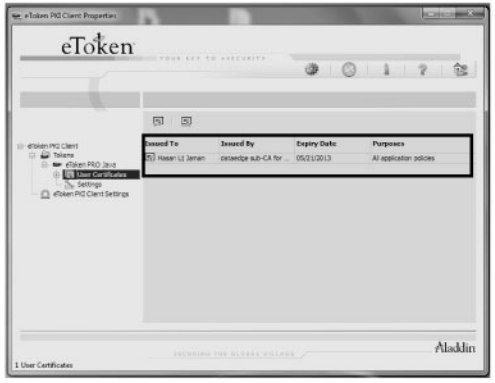
টোকেনটির ড্রাইভার ইনস্টল হলে এবং টোকেনটি ইউএসবি পোর্টে সংযুক্ত করা হলে আপনি অপারেটিং সিস্টেমের টাস্কবারে তা দেখতে পাবেন (চিত্র-৮৮)।

চিত্র-৮৮

টাস্কবারের গোলাকার চিহ্নিত আইকনটির উপর দুইবার ক্লিক করলে একটি উইন্ডো খুলবে এবং বাম দিকে ট্রি (Tree) আকৃতির তথ্যাদি দেখা যাবে (চিত্র-৮৯)।

চিত্র-৮৯

মাউস ক্লিকের মাধ্যমে ট্রি (Tree) প্রসারিত করলে certificate/user certificates নামে বাক্য দেখা যাবে। user certificates-এ ক্লিক করলে ডান দিকে টোকেনে সংরক্ষিত সার্টিফিকেট প্রদর্শিত হবে (চিত্র-৯০)।



চিত্র-৯০

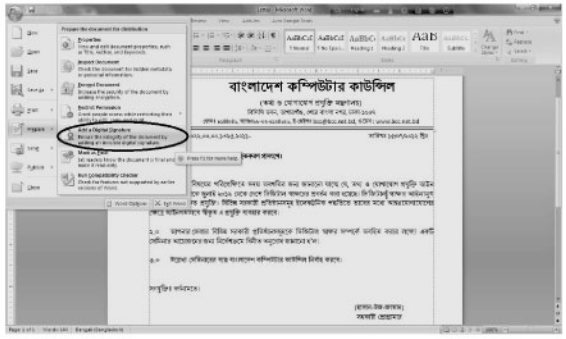
আপনি ইচ্ছা করলে সার্টিফিকেটের উপর ক্লিক করে বিস্তারিত তথ্য দেখতে পারেন (চিত্র-৯১)।

চিত্র-৯১

হার্ড টোকেন ব্যবহারের ক্ষেত্রে কোনরকম সার্টিফিকেট install এর দরকার পড়ে না। যখন দরকার তখন টোকেনটি কম্পিউটারে সংযুক্ত করে তাৎক্ষণিকভাবে স্বাক্ষর প্রয়োগ করা যায়। সিএ আপনার টোকেনটি সার্টিফিকেটসহ ব্যবহারোপযোগী করে PIN/Password যুক্ত অবস্থায় আপনাকে হস্তান্তর করবে অথবা সিএ'র ওয়েবসাইট থেকে ডাউনলোড করার সময় টোকেনে ডাউনলোড নির্বাচন করলে সরাসরি টোকেনে সার্টিফিকেট Import হয়ে যাবে।

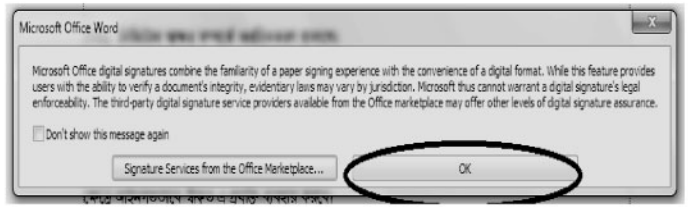
(ক) ডকুমেন্টে ডিজিটাল স্বাক্ষর সংযোজন

টোকেনের মাধ্যমে ডকুমেন্টে ডিজিটাল স্বাক্ষর প্রয়োগের ক্ষেত্রে এ নির্দেশিকায় মাইক্রোসফট অফিস ২০০৭ ব্যবহার করা হয়েছে। ধরা যাক, আপনি যে ডকুমেন্টটি ডিজিটাল স্বাক্ষরযুক্ত করতে চাচ্ছেন, সেটি আপনার সামনে খোলা এবং প্রস্তুত অবস্থায় আছে। স্বাক্ষর করার জন্য অফিস বাটনে ক্লিক করলে একটি মেনু দেখা যাবে, সেখানে Prepare নামে মেনু আইটেমের উপর ক্লিক করলে, আরেকটি সাব-মেনু খুলবে। সেখানে 'Add Digital Signature' অপশনের উপর ক্লিক করুন (চিত্র-৯২)।



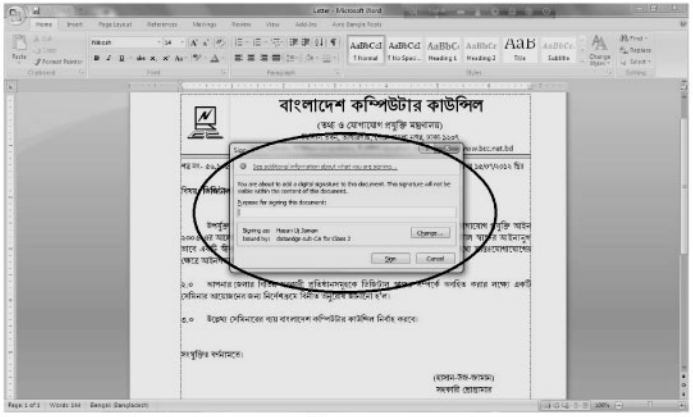
চিত্র-৯২

ক্লিক করা হলে একটি মেসেজ বক্স (চিত্র-৯৩) প্রর্দশিত হবে; Ok বাটনে ক্লিক করুন।



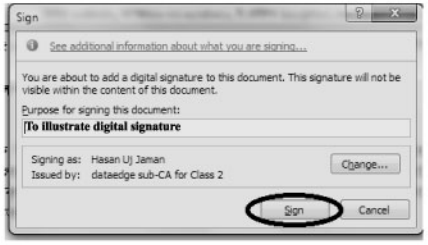
চিত্র-৯৩

এটি স্বয়ংক্রিয়ভাবে USB পোর্টে সংযুক্ত হার্ড টোকেনটি থেকে আপনার ডিজিটাল সার্টিফিকেটটি ব্যবহার করতে চাইবে (চিত্র-৯৪)।



চিত্র-৯৪

টেক্সট বক্সে স্বাক্ষর করার কারন লিখুন (ঐচ্ছিক)। তারপর Sign বাটনটিতে ক্লিক করুন (চিত্র-৯৫)।

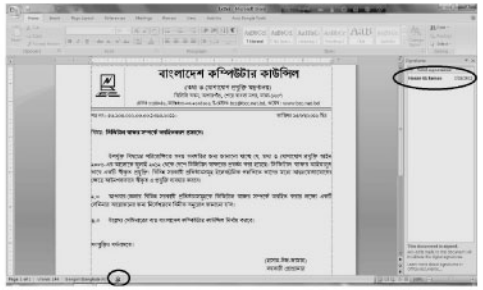


চিত্র-৯৫

এখন আপনাকে আপনার PIN/Password কোডটি লিখতে হবে (চিত্র-৯৬)। Ok বাটনে ক্লিক করুন।

চিত্র-৯৬

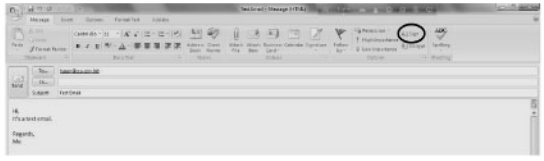
আপনার ডকুমেন্টটি ডিজিটাল স্বাক্ষরযুক্ত হয়ে গেলো। ডকুমেন্টের নিচের দিকে লাল রিবনযুক্ত চিহ্ন প্রর্দশিত হবে এবং ডান দিকে ডিজিটাল স্বাক্ষর সংক্রান্ত তথ্য দেখাবে (চিত্র-৯৭)।



চিত্র-৯৭

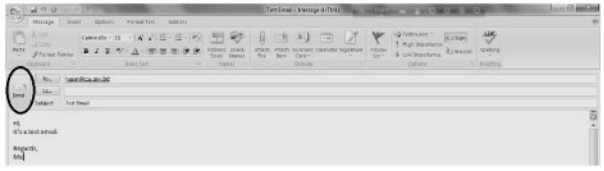
(খ) মেইলে ডিজিটাল স্বাক্ষর প্রয়োগ

আউটলুক ২০০৭ খুলুন এবং একটি মেইল তৈরি করুন। উপরে ডান দিকে রিবন টুলবারে Sign নামে একটি আইকন দেখা যাবে। মাউস ক্লিকের মাধ্যমে এটি নির্বাচিত করুন (চিত্র-৯৮)।



চিত্র-৯৮

এখন বাম দিকের Send বাটনে ক্লিক করুন (চিত্র-৯৯)।

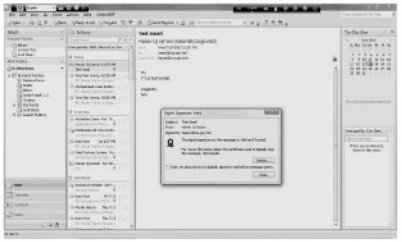


চিত্র-৯৯

USB পোর্টে টোকেনটি সংযুক্ত থাকলে আউটলুক আপনার মেইলটি পাঠানোর পূর্বে টোকেনের PIN/Password চাইবে (চিত্র-১০০)। PIN/Password দিয়ে Ok বাটনে ক্লিক করুন।

চিত্র-১০০

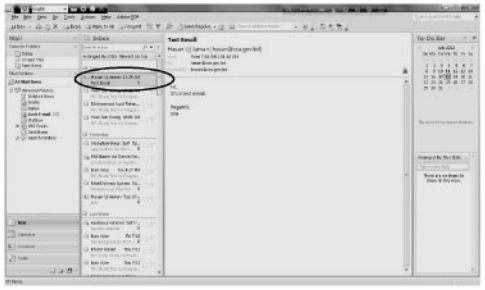
আপনার মেইলটি ডিজিটাল স্বাক্ষরযুক্ত হয়ে গেল। আউটলুক এডিটরে Send ফোল্ডার থেকে ইতোপূর্বে প্রেরিত মেইলটি নির্বাচিত করলে লাল রিবন চিহ্ন দেখা যাবে। ক্লিক করলে স্বাক্ষরের অবস্থা, বৈধতা ইত্যাদি দেখা যাবে (চিত্র-১০১)।



চিত্র-১০১

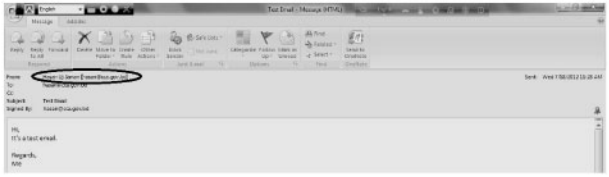
(গ) মেইল এনক্রিপশন পদ্ধতি

মেইল এনক্রিপ্ট করার জন্য প্রথমে প্রাপকের সার্টিফিকেটটি আপনার আউটলুক অ্যাড্রেসবুকে যুক্ত করতে হবে। আউটলুক অ্যাড্রেসবুকে প্রাপকের পাবলিক কী সংযুক্ত করার জন্য প্রাপকের ডিজিটাল স্বাক্ষরযুক্ত কোন একটি মেইল নির্বাচিত করুন। মাউস দিয়ে তা ডাবল ক্লিক করুন (চিত্র-১০২)।



চিত্র-১০২

মেইলটি নতুন একটি উইন্ডোতে দেখা যাবে (চিত্র-১০৩)। যেখানে প্রাপকের নাম From হিসাবে দেখা যাবে। মাউসটি নামের উপর রেখে ডান বাটনে ক্লিক করুন।

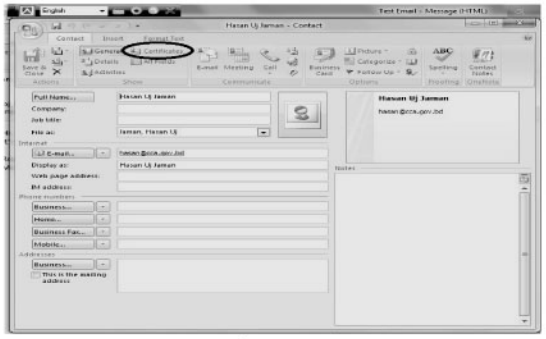


চিত্র-১০৩

ফলে একটি মেনু খুলবে (চিত্র-১০৪), সেখানে Add To Outlook Contacts অপশনটির উপর ক্লিক করুন।

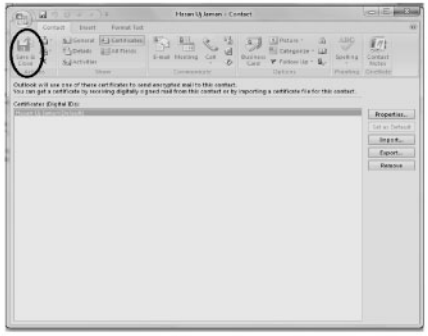
চিত্র-১০৪

একটি নতুন উইন্ডো খুলবে, সেখানে রিবন টুলবারে Certificates আইকনের উপর ক্লিক করুন (চিত্র-১০৫)



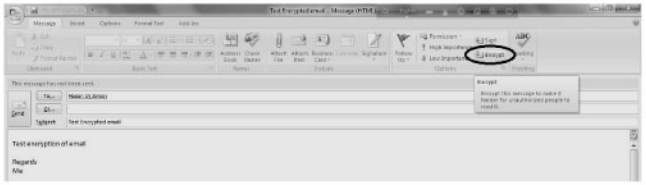
চিত্র-১০৫

ফলে প্রাপকের সার্টিফিকেটটি প্রর্দশিত হবে। এখন উপরে বাম দিকে Save & Close বাটনে ক্লিক করুন (চিত্র-১০৬)।



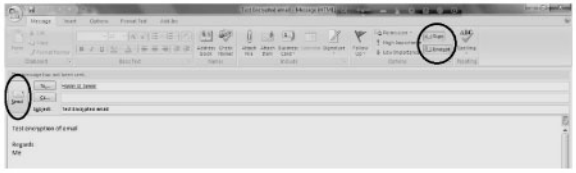
চিত্র-১০৬

এখন একটি নতুন মেইল লিখুন। এডিটরের রিবন টুলবারে Encrypt আইকনটিকে নির্বাচিত করুন (চিত্র-১০৭)।



চিত্র-১০৭

চাইলে আপনি Sign আইকনটিও নির্বাচিত করতে পারেন, সেক্ষেত্রে আপনার মেইলটি স্বাক্ষরযুক্ত এবং এনক্রিপ্টেড অবস্থায় যাবে। এখন Send বাটনে ক্লিক (চিত্র-১০৮) করুন।

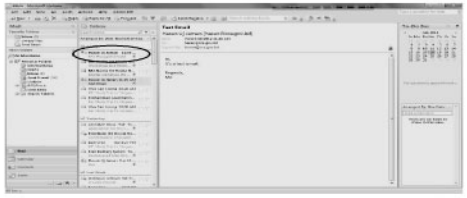


চিত্র-১০৮

আউটলুক মেইলটি পাঠানোর পূর্বে একইভাবে আপনার টোকেনের PIN/Password চাইবে (চিত্র-১০৯)। PIN/Password দিয়ে Ok বাটনে ক্লিক করুন।

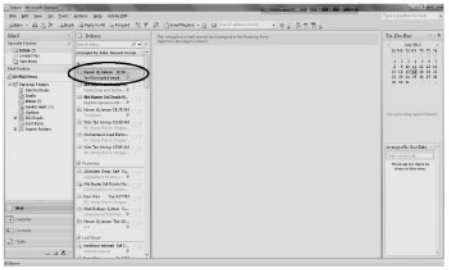
চিত্র-১০৯

আপনার মেইলটি এনক্রিপ্টেড অবস্থায় প্রেরিত হল। প্রাপকের আউটলুকে মেইলটি নীল রঙের তালা আইকনযুক্ত অবস্থায় দেখা যাবে (চিত্র-১১০)।



চিত্র-১১০

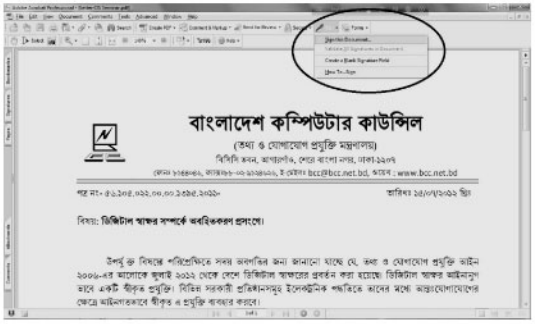
মেইলটি ডিক্রিপ্ট করার জন্য প্রাপকের ব্যক্তিগত কী (Private key) দরকার পড়বে। প্রাপক যদি তার ক্রিপটো টোকেনটি USB পোর্টে সংযুক্ত না করেন, তাহলে মেইলটি পড়তে পারবেন না (চিত্র-১১১)।



চিত্র-১১১

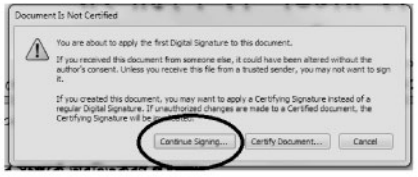
(ঘ) পিডিএফ ডকুমেন্ট স্বাক্ষর পদ্ধতি

প্রথমে একটি পিডিএফ ডকুমেন্ট খুলুন। টুলবারে Sign আইকনটির উপর ক্লিক করুন, নতুন একটি মেনু খুলবে। সেখানে Sign This Document অপশনটিতে ক্লিক করুন (চিত্র-১১২)।



চিত্র-১১২

ফলে একটি ডায়ালগ বক্স (চিত্র-১১৩) আসবে, সেখানে Continue Signing বাটনে ক্লিক করুন।



চিত্র-১১৩

আরেকটি ডায়ালগ বক্স খুলবে, যেখানে আপনাকে ডকুমেন্টটি ডিজিটাল স্বাক্ষর এর স্থান নির্ধারণ সংক্রান্ত পদ্ধতি নির্বাচিত করতে হবে (চিত্র-১১৪)। Next বাটনে ক্লিক করুন।

চিত্র-১১৪

একটি মেসেজ প্রর্দশিত হবে (চিত্র-১১৫)। Ok বাটনে ক্লিক করুন।

চিত্র-১১৫

আপনি যখন PDF ডকুমেন্টে সিগনেচার ফিল্ড তৈরি করে ফেলবেন, তখন একটি ডায়ালগ বক্স (চিত্র-১১৬) দেখা যাবে।

চিত্র-১১৬

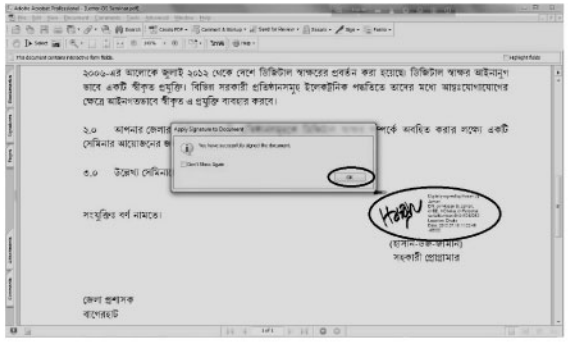
ঐচ্ছিক তথ্যাদি দেওয়ার পর, Sign and Save বাটনে ক্লিক করুন (চিত্র-১১৭)।

চিত্র-১১৭

Acrobat Reader এখন আপনার টোকেনটির Pin/Password চাইবে। Pin/Password লিখুন এবং Ok বাটনে ক্লিক করুন (চিত্র-১১৮)।

চিত্র-১১৮

একটি সফলবার্তা প্রদর্শিত হবে। Ok বাটনে ক্লিক করুন। আপনার পিডিএফ ডকুমেন্টটি স্বাক্ষরযুক্ত হয়ে গেল (চিত্র-১১৯)।



চিত্র-১১৯

৫. উপসংহার

এ ব্যবহারিক নির্দেশিকায় ডিজিটাল স্বাক্ষর প্রয়োগের নিতান্তই মৌলিক ব্যবহারবিধি বর্ণনা করা হয়েছে, যা অফিস বা মেইল ক্লায়েন্ট সফটওয়্যার ব্যবহার করেই প্রয়োগ করা সম্ভব। ব্যবহারকারী যদি কাস্টমাইজড সফটওয়্যারে ডিজিটাল স্বাক্ষর সার্টিফিকেট ব্যবহার করতে চান, সেক্ষেত্রে ঐ কাস্টমাইজড সফটওয়্যারে ডিজিটাল স্বাক্ষর প্রয়োগ পদ্ধতি জেনে নিতে হবে এবং প্রয়োগ করতে হবে। আশা করা যায় যে, এ নির্দেশিকাটি দেশে ডিজিটাল স্বাক্ষর এর ব্যবহার প্রসারে একটি সহায়ক দলিল হিসেবে গণ্য হবে।