১. সত্যিকার অর্থে ডিজিটাল স্বাক্ষর কি?

উত্তরঃ সাধারনত হস্তলিখিত কোন স্বাক্ষরকে স্ক্যান করে কোন প্রিন্টেড ডকুমেন্টে সংযুক্ত করার মাধ্যমে ধরে নেওয়া হয় উক্ত ডকুমেন্ট যথাযথ প্রেরকের কাছ হতে উৎপত্তি হয়েছে ।সত্যিকার অর্থে এটি ডিজিটাল স্বাক্ষর নয়। ডিজিটাল স্বাক্ষর ইলেক্ট্রনিক মেসেজ এর মত একই কার্য সম্পাদন করে। ডিজিটাল স্বাক্ষর হল একটি মেসেজ ডাইজেস্টে'র এনক্রিপ্টেড ভার্সন যা একটি মেসেজ'র সাথে একত্রে সংযুক্ত থাকে। একটি নিরাপদ ডিজিটাল স্বাক্ষর দু'টি অংশ নিয়ে গঠিতঃ

- নিজের জন্য গোপনীয় চাবি (প্রাইভেট কী), যা দ্বারা ডিজিটাল স্বাক্ষর সৃষ্টি করা হয়।
- সবার জন্য উন্মোচনের চাবি (পাবলিক কী), যা দ্বারা ডিজিটাল স্বাক্ষর যাচাই করা হয়।

একটি ডকুমেন্টে ডিজিটাল স্বাক্ষর ব্যবহার পদ্ধতিতে যেকোন জালিয়াতি ধরা সম্ভব এবং এ পদ্ধতিতে যথাযথ ব্যক্তি দ্বারা স্বাক্ষরিত হয়েছে কিনা তা সহজেই যাচাই করা যায়। দু'টি চাবি যেমনঃ সবার জন্য উন্মোচনের চাবি (পাবলিক কী) এবং নিজের জন্য গোপনীয় চাবি (প্রাইভেট কী) দ্বারা ডিজিটাল স্বাক্ষর পদ্ধতি সম্পন্ন হয়। প্রেরক যে দলিল পাঠাবেন তা কম্পিউটার প্রোগ্রাম ব্যবহার করে হ্যাশ তৈরী করেন, তারপর তার গোপনীয় চাবি দিয়ে উক্ত হ্যাশটিকে ডিজিটাল স্বাক্ষরে পরিণত করেন। তারপর স্বাক্ষর যুক্ত দলিল প্রাপকের কাছে পাঠিয়ে দেন।

প্রাপক কম্পিউটার প্রোগ্রাম দ্বারা প্রাপ্ত দলিলকে হ্যাশে পরিণত করেন এবং প্রেরকের পাবলিক চাবি দ্বারা স্বাক্ষর থেকেও হ্যাশ বের করেন। দুইটি হ্যাশ এক হলে শনাক্তকরণ নিশ্চিত হয়।

এভাবেই ডিজিটাল স্বাক্ষরের মাধ্যমে নিরাপদে দলিল প্রেরিত হয়।

২. ডিজিটাল সার্টিফিকেট কি?

উত্তরঃ ডিজিটাল সার্টিফিকেট হল কাগজের সার্টিফিকেটের সমতুল্য একটি ইলেক্ট্রনিক ফরম্যাট। কাগজের সার্টিফিকেট যেমনঃ পাসপোর্ট, লাইসেন্স অথবা মেম্বারশীপ কার্ড দ্বারা কোন ব্যক্তি নির্দিষ্ট কোন উদ্দেশ্যে নিজের পরিচিতি প্রদান করেন।তেমনি একটি ডিজিটাল সার্টিফিকেট দ্বারা ইন্টারনেটে ইলেক্ট্রনিক্যালি উপস্থাপনার মাধ্যমে কোন ব্যক্তি নির্দিষ্ট কোন উদ্দেশ্যে নিজের পরিচিতি প্রদান করেন।

৩. সার্টিফাইং অথোরিটিজ (সিএ) কি?

উত্তরঃ একটি বিশ্বস্ত তৃতীয় পক্ষ যা একটি সংস্থা বা কোম্পানী যারা ডিজিটাল স্বাক্ষর এবং পাবলিক কী ও প্রাইভেট কী সৃষ্টি করার মাধ্যমে গ্রাহকদের ডিজিটাল সার্টিফিকেট প্রদান করে থাকে। সিএ'দের মূল ভমিকা হল একজন ব্যক্তির জন্য স্বতন্ত্র সার্টিফিকেট প্রদানের নিশ্চয়তা দেওয়া। ই-কমার্সে দুই পক্ষের তথ্য নিরাপত্তা এবং আর্থিক লেনদেনের ক্ষেত্রে সিএরা নির্দিষ্ট ব্যক্তির পরিচতি প্রদানে নিশ্চয়তা দেয়।

সার্টিফিকেট প্রদানের উদ্দেশ্যে সিএ দু' ধরনের হতে পারে- একটি হল স্ংস্থার নিজস্ব কর্মকান্ড পরিচালনার জন্য, অপরটি হল সংস্থার বাহিরে সকলের জন্য।

৪. ডিজিটাল সার্টিফিকেটের কাজ কি?

উত্তরঃ ডিজিটাল সার্টিফিকেটের মাধ্যমে কোন ব্যক্তির পরিচিতি যাচাই করা হয়। এটি দ্বারা স্বাক্ষর প্রদানকারীর পরিচিতি পাওয়ার মাধ্যমে প্রাপকের আত্মবিশ্বাস বৃদ্ধি পায় যে প্রাপ্ত দলিলে কোনরুপ জালিয়াতি বা পরিবর্তন ঘটেনি। ওয়েব সাইটের কন্ট্রোল এক্সেস, ভার্চুয়াল প্রাইভেট নেটওয়ার্ক তৈরীতে, ই-মেইল নিরাপত্তায় এবং ডাউনলোডকৃত সফটওয়্যরের সঠিকতার নিশ্চয়তা প্রদানে ডিজিটাল সার্টিফিকেট ব্যবহার করা হয়।

৫. ডিজিটাল সার্টিফিকেটে কি কি বিষয়বস্তু আছে?

উত্তরঃ ডিজিটাল সার্টিফিকেটে ৩ (তিন) টি উপাদান আছেঃ যেমন-

ক. বিষয়ের নাম এবং অন্য সার্টিফিকেট এক্সটেনশনঃ ব্যক্তির নাম, জাতীয়তা, ই-মেইল এড্রেস, সংস্থার নাম, বিভাগ, ছবি, ফিংগার প্রিন্ট, পাসপোর্ট নম্বর ইত্যাদি।

খ. পাবলিক কী ইনফরমেশনঃ পাবলিক কীতে উপরোক্ত ব্যক্তিগত তথ্যগুলো বিদ্যমান থাকে।পাবলিক কী একটি এসিম্যেট্রিক কী হতে পারে কিন্তু এটি সাধারনত একটি আরএসএ কী।

গ. সার্টিফাইং অথোরিটি স্বাক্ষরঃ সিএ উপরোক্ত দু'টি উপাদানকে স্বাক্ষর করে সার্টিফিকেটের নিশ্চয়তা প্রদান করে।প্রাপক স্বাক্ষর যাচাই করে জানতে পারবে যে কোন সিএ কর্তৃক প্রেরকের সার্টিফিকেট প্রদান করা হয়েছে।

৬. ডিজিটাল সার্টিফিকেট কত ধরনের?

উত্তরঃ ডিজিটাল সার্টিফিকেট দুই ধরনের হতে পারে- সার্ভার সার্টিফিকেট ও ব্যক্তিগত সার্টিফিকেট। কি ধরনের তথ্য এবং কার পরিচিতি- এ দুই ক্ষেত্রে সার্টিফিকেটদ্বয়ের পার্থক্য পরিলক্ষিত হয়। যেমনঃ সার্ভার সার্টিফিকেটে হোস্ট নাম এবং ব্যক্তিগত সার্টিফিকেটে ব্যক্তির পুরো নাম থাকবে।

৭. ব্যক্তিগত সার্টিফিকেট কি?

উত্তরঃ ব্যক্তিগত সার্টিফিকেটে কোন ব্যক্তির পরিচিতি প্রদান করে।এতে ব্যক্তির পুরো নাম, ব্যক্তিগত বিভিন্ন বিষয় উল্লেখ থাকে। ই-মেইল নিরাপত্তায়, গুরুত্বপূর্ণ তথ্যে প্রবেশাধিকার নিয়ন্ত্রণে ব্যক্তিগত সার্টিফিকেট ব্যবহার করা হয়।

৮. সার্ভার সার্টিফিকেট কি?

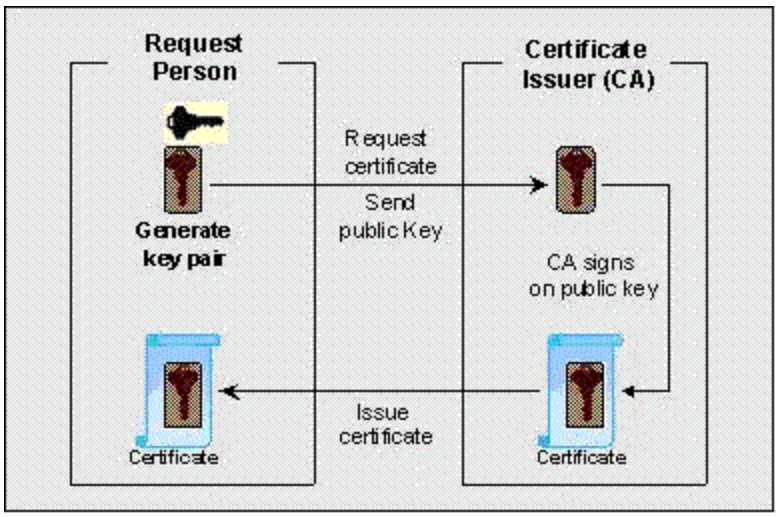
উত্তরঃ সার্ভার সার্টিফিকেট দ্বারা একটি সার্ভার (কম্পিউটার) সনাক্ত করে। অতএব, একজন ব্যক্তির নামের পরিবর্তে সার্ভার সার্টিফিকেট হোস্টনেম ধারণ করে যেমন www.cca.gov.bd সার্ভার সার্টিফিকেট নিরাপদে অন লাইন লেনদেন নিশ্চিত করার জন্য ব্যবহার করা হয়।

৯. তথ্য গোপনীয়তা কি?

উত্তরঃতথ্য গোপনীয়তা বলতে এমন একটি অবস্থা বোঝায় যে একটি বার্তাকে প্রাপক ছাড়া অন্য কেউ পড়তে পারবেনা। এনক্রিপশন ও ডিক্রিপশন গোপনীয়তা নিশ্চিত করে।

১০. কিভাবে ডিজিটাল সার্টিফিকেট জারি হয়?

উত্তরঃ চিত্রে CA দ্বারা জারিকৃত একটি সার্টিফিকেটের জন্য অনুরোধ এবং প্রদান প্রক্রিয়া দেখানো হলঃ



সার্টিফিকেট আবেদনকারী অবশ্যই তার নিজের কী জোড়া এবং তার সনাক্তকারী প্রমান সহ সিএকে পাঠাতে হবে। সিএ নতুন সার্টিফিকেটে পাবলিক কী স্থাপন করবে, সংশ্লিষ্ট প্রাইভেট-কি ব্যবহার করে সার্টিফিকেটটি ডিজিটালি স্বাক্ষরিত হবে এবং তারপর আবেদনকারীকে সার্টিফিকেটটি পাঠাবে। দ্রষ্টব্য: সিএ সার্টিফিকেট আবেদনকারীর সনাক্তকরণ পরীক্ষা করে সার্টিফিকেট সৃষ্টি করবে। বিভিন্ন সি এ বিভিন্নভাবে সনাক্তকরণ যাচাই করে সার্টিফিকেট জারি করবে। যেমন একজন সিএ পরিচয়পত্র দেখে যাচাই করবে, অন্যজন যথাযথ কর্তৃপক্ষের অনুমোদিত সনদের সাপেক্ষে যাচাই করবে।

১১. পিকেআই বলতে কী বোঝায়?

উত্তরঃ পিকেআই হল ইন্টারনেটে সার্টিফিকেট ব্যবহারকারীর সনাক্তকরনের সামগ্রিক ব্যবস্থা। ডিজিটাল সার্টিফিকেট জারি এবং এর বৈধতা যাচাই করার জন্য প্রত্যয়নকারী কর্তৃপক্ষ দায়ী থাকবে। যোগাযোগ বা ব্যবসার ক্ষেত্রে নেটওয়ার্কে প্রমাণীকরণ, বিশ্বস্ততা, সততা ও স্বীকৃতি এর মত নিরাপদ সেবা প্রদানের উদ্দেশ্যে এটি কাজ করে।

১২. পিকেআই এর উপাদানগুলো কি কি?

উত্তরঃ পিকেআই উপাদানগুলো হচ্ছেঃ

- <u>সার্টিফিকেট প্রদানকারী কর্তৃপক্ষঃ</u> সার্টিফিকেট প্রদানকারী কর্তৃপক্ষ সার্টিফিকেট জারি এবং বাতিল করেন। এটা নিশ্চয়তা প্রদান করে যে সার্টিফিকেট ব্যবহারকারীর প্রত্যায়িত সকল তথ্য সঠিক । সি এ রা প্রবিধান মোতাবেক কর্মকান্ড সম্পাদন করেন। সার্টিফিকেট প্রদানকারী কর্তৃপক্ষ হিসাবে সিএ সার্টিফিকেট ম্যানেজমেন্ট সিস্টেম এর কাজ এবং নির্ধারিত সময় অন্তর CRL বিতরণ করে গুরুত্বপূর্ণ ভূমিকা পালন করে। তারা কোনরুপ ঝুঁকি ছাড়াই নিরীক্ষা করতে সক্ষম।

- সার্টিফিকেট সংগ্রহস্থলঃ সার্টিফিকেট সংগ্রহস্থল সার্টিফিকেট এবং সিআরএল তথ্য সংরক্ষণ করার জন্য ব্যবহার হয়। এটা সার্টিফিকেট সম্পর্কে সর্বশেষ তথ্য প্রাপ্তির জন্য ব্যবহার করা হয়। সিআরএল হল বাতিলকৃত সার্টিফিকেটের একটি তালিকা। প্রত্যেকটা তালিকা সিএ কর্তৃক ডিজিটালরূপে স্বাক্ষরিত। সার্টিফিকেট এবং CRL অনুসন্ধান করার জন্য ব্যবহারকারী সার্টিফিকেট সংগ্রহস্থল ব্যবহার করে থাকে।

- এন্ড ইউজারঃ এন্ড ইউজার হল যে সাধারণত একটি পিসি থেকে ইন্টারনেটের মাধ্যমে পিকেআই এনাবেল সার্ভিস ব্যবহার করে। এই সেবায় নিরাপদ ই-মেইল অন্যগুলোর মধ্যে একটি। প্রাপকের পাবলিক কী ব্যবহার করে মেইলটি এনক্রিপ্ট করা হয়। প্রাপক তারপর প্রেরকের স্বাক্ষর যাচাই করতে পারে। একটি গুরুত্বপূর্ণ মেইল আদান-প্রদানে স্বীকৃতি , প্রমাণীকরণ, সততা এবং গোপনীয়তার উদ্দেশ্য ব্যবহারকারী এবং সেবা প্রদানকারীর মধ্যে একটি আইনত বাধ্যতামূলক চুক্তি করা হয়।

সেবা প্রদানকারীঃ সেবা প্রদানকারী বলতে ইমেইল সেবা বা কোন পিকেআই ভিত্তিক সেবা বোঝায়। সেবা প্রদানকারী সর্বশেষ এনটিটি সার্ভার অ্যাক্সেস করার সময় অবাঞ্ছিত প্রচেষ্টা প্রতিরোধ করতে ফায়ারওয়ালের মাধ্যমে নিরাপত্তা ব্যবস্থা গঠন করে। শেষ ব্যবহারকারী এবং সর্বশেষ এনটিটির নিজেদের মধ্যে অনুমোদনের পর নিরাপত্তা সেবা শুরু করে। এই দু'সত্তার মধ্যে তথ্য এনক্রিপ্টেড অবস্থায় পরিবহন হয় যাতে ডাটা সঞ্চালনের সময় উভয় পক্ষের গোপনীয়তা নিশ্চিত হয়।

১৩. পিকেআই প্রক্রিয়াগুলো কি কি?

উত্তরঃ পিকেআই প্রক্রিয়াগুলো হলোঃ

সার্টিফিকেট প্রদানঃ সিএরা নির্ধারিত নীতিমালা অনুযায়ী ব্যবহারকারীদের এবং শেষ সত্ত্বাকে সার্টিফিকেট জারি করে। সিএ প্রত্যায়িত পাবলিক কী এবং সংশ্লিষ্ট প্রাইভেট কী যুক্ত করে সার্টিফিকেট জারি করে। সিএ যে সার্টিফিকেট জারি করে সে সার্টিফিকেটের সকল তথ্য অবশ্যই সঠিক হতে হবে যাতে একটি স্বতন্ত্র তৃতীয় পক্ষ এটি যাচাই করতে পারে। সার্টিফিকেট সাধারণত নির্দিষ্ট উদ্দেশ্যের উপর নির্ভর করে একটি স্বল্প সময়ের জন্য সার্টিফিকেট জারি করা হয়।

সার্টিফিকেট প্রত্যাহারঃ একটি সার্টিফিকেটের সাথে একটি ব্যক্তিগত কী যুক্ত করার পরও যদি তা উন্মুক্ত হওয়া বা উন্মুক্ত করা হয়েছে বলে হুমকির সম্মুখীন হয়, তখন সার্টিফিকেটের মালিক এ বিষয়টি সিএকে জানাবে। সিএ দ্বারা স্বাক্ষরিত সার্টিফিকেটটি সার্টিফিকেট প্রত্যাহার তালিকা (সিআরএল) নামক তালিকায় স্থাপন করা হয়। সিআরএল তালিকা নিয়মিতভাবে প্রকাশিত হয় এবং যা সহজেই প্রবেশযোগ্য । ফলে প্রত্যাহারিত সার্টিফিকেটটি গ্রহণ করা উচিত নয় এটি সহজেই বোঝা যায়।

প্রমাণীকরণ / যাচাইঃ কোন পক্ষ লেনদেনে জড়িত হলে তা রেসপন্স মেকানিজমের মাধ্যমে প্রমান করা যেতে পারে। ব্যবহারকারী তার নিজের সার্টিফিকেটের মাধ্যমে চ্যালেঞ্জ সহকারে তা প্রমান করতে পারে যা প্রাইভেট কী দ্বারা এনক্রিপ্টেড

থাকে। তারপর চ্যালেঞ্জিং পার্টি সার্টিফিকেটের মধ্যে থাকা পাবলিক কী ব্যবহার করে তা ডিক্রিপ্ট করে ব্যবহারকারীর সার্টিফিকেটটি অনুমোদিত বলে মনে করে। উভয় রেসপন্স যাচাই করে মিলে যাওয়ার মাধ্যমে উভয় পক্ষের অর্থাৎ ক্লায়েন্ট এবং সার্ভার প্রান্তের প্রমানীকরন সম্পন্ন হয়। ব্যবহারকারীরা এই সমগ্র প্রক্রিয়ায় বিশ্বস্ততার সহিত লেনদেন করার ক্ষেত্রে সার্টিফিকেট প্রদানকারী খুব গুরুত্বপূর্ণ ভূমিকা পালন করে।

স্বীকৃতি / যাচাইঃ স্বীকৃতি সেবা গুরুত্বপূর্ণ চূড়ান্ত চুক্তি স্বাক্ষর, ব্যবসায়িক লেনদেন, মেইল ইত্যাদিতে ব্যবহার করা হয়। যদি প্রাইভেট কী রক্ষিত থাকে, তাহলে ডিজিটাল স্বাক্ষর কপি করা অসম্ভব। যে কোন পার্টি সিএ কর্তৃক ইস্যু করা সার্টিফিকেট যাচাই করতে পারে। মূল তথ্যের সাথে প্রদত্ত প্রাইভেট কী দ্বারা এনক্রিপ্ট করে ডিজিটাল স্বাক্ষর নির্মিত হয়। প্রাপক প্রত্যায়িত পাবলিক কী ব্যবহার করে কাংখিত মান মিলিয়ে যাচাই করবে। এই যাচাই পদ্ধতি সম্পাদনের সময় প্রাপকের নিশ্চিত হওয়া প্রয়োজন যে সার্টিফিকেটের মেয়াদ এবং প্রত্যাহার অবস্থায় আছে কিনা ।

১৪. ক্রিপ্টোগ্রাফি (সংকেতলিপি) কি?

উত্তরঃ ক্রিপ্টোগ্রাফি হল প্রেরক এবং এক বা একাধিক প্রাপকদের মধ্যে নিরাপদ যোগাযোগের একটি সক্রিয় বিজ্ঞান। প্রেরক একটি বার্তাকে এনক্রিপ্টেড (কম্পিউটার প্রোগ্রাম এবং একটি গোপন কী সহ) করে পাঠায় এবং প্রাপক উক্ত বার্তাকে ডিক্রিপ্টেড (যা একই কম্পিউটার প্রোগ্রাম এবং একটি কী সহ যা প্রেরকের একই কী হতে পারে অথবা পারে না) অবস্থায় গ্রহন করে। ক্রিপ্টোগ্রাফি দুই ধরনেরঃ গোপন / সিমেট্রিক কী ক্রিপ্টোগ্রাফি এবং পাবলিক / এসিমেট্রিক কী ক্রিপ্টোগ্রাফি। ক্রিপ্টোগ্রাফির বৈশিষ্ট্য হল তথ্য গোপনীয়তা, তথ্য অখন্ডতা , প্রেরক প্রমাণীকরণ, এবং স্বীকৃতি।

১৫. কী(চাবি) কাকে বলে?

উত্তরঃ সত্যিকারে কী(চাবি) ব্যবহার করা হয় তালা খোলা এবং বন্ধ করার জন্য। ক্রিপ্টোগ্রাফির কাজও একই যেমনঃ এনক্রিপশন ও ডিক্রিপশন। এই ক্ষেত্রে কী হল একটি আলগোরিদিমিক প্যাটার্ন বা নিয়ম যাতে বার্তাটি অপাঠ্য অবস্থায় থাকে।

১৬. এনক্রিপশন কি?

উত্তরঃ এনক্রিপশন হল কোন বার্তাকে অপাঠ্য ফর্ম থেকে পাঠযোগ্য ফর্মে রূপান্তর করা।

১৭. ডিক্রিপশন কি?

উত্তরঃ ডিক্রিপশন হল এনক্রিপশন এর বিপরীত। এটি এনক্রিপ্ট করা তথ্যকে বোধযোগ্য ফর্মে ফিরিয়ে আনে।

১৮. মেসেজ ডাইজেস্ট কি?

উত্তরঃ মেসেজ ডাইজেস্ট বলতে,একটি মেসেজের হ্যাশকে বোঝায়, এনক্রিপশনের সময় বার্তাটির উপর নির্দিষ্ট গাণিতিক গণনা (হ্যাশ ফাংশন) সম্পাদনের ফলাফল থেকে প্রাপ্ত তথ্যকে বোঝায়। বার্তাটির দুই ধরনের বৈশিষ্ট্য নিম্নে দেওয়া হলঃ

- মূল বার্তার একটি ছোট পরিবর্তন হলে মেসেজ ডাইজেস্টের বড় পরিবর্তন হয়ে থাকে।

- মেসেজ ডাইজেস্ট থেকে মূল বার্তা আহরণ করা সম্ভব নয়। এটা বার্তার "ফিঙ্গারপ্রিন্ট" হিসাবে কাজ করে এবং তথ্য অখন্ডতা নিশ্চিত করার জন্য ব্যবহার করা হয়।

১৯. তথ্য অখন্ডতা (ডাটা ইনটিগ্রিটি) কি?

উত্তরঃ প্রাপক যে বার্তা পায় যদি তা ঠিক যেভাবে পাঠানো হয়েছে তা হয় অর্থাৎ ট্রান্সমিশনের সময় বার্তা অবিকৃত হয় তাকে তথ্য অখন্ডতা বলা হয়।

২০. প্রেরক প্রমাণীকরণ কি?

উত্তরঃ প্রেরক প্রমাণীকরণ হল একটি বার্তা নির্দিষ্ট প্রেরক ছাড়া অন্য কারও থেকে উদ্ভূত হয়নি তা নিশ্চিত করার একটি প্রক্রিয়া। ডিজিটাল স্বাক্ষর এবং ডিজিটাল সার্টিফিকেটের মাধ্যমে প্রেরকের প্রমাণীকরণ সম্পন্ন হয়।

২১. মূল তথ্য স্বীকৃতি / তথ্য জবাবদিহিতা কি?

উত্তরঃ তথ্য জবাবদিহিতা হল সঠিক যে জায়গা হতে বার্তা পাঠানো হয়েছে তার প্রমাণকে বোঝায়। প্রেরক এটা অস্বীকার করতে পারবে না। এটি ডিজিটাল স্বাক্ষরের মাধ্যমে সম্পন্ন করা হয়।

২২. কেন ডিজিটাল সার্টিফিকেট এর বিষয়বস্তু বিশ্বাস করা উচিত?

উত্তরঃ যেকারনে আমরা একটি ড্রাইভার লাইসেন্স বিশ্বাস করি: যথাযথ কর্তৃপক্ষের (পরিবহন দপ্তর) ফর্গ স্বাক্ষর বা অনুমোদিত স্ট্যাম্প দ্বারা পৃষ্ঠাঙ্কন করে সংযুক্ত করা হয় বলে । প্রত্যয়নকারী কর্তৃপক্ষ বা সিএ যারা আইন দ্বারা ক্ষমতাপ্রাপ্ত একটি স্বাধীন এবং বিশ্বস্ত কর্তৃপক্ষ তারা অনুরূপ পদ্ধতিতে ডিজিটাল সার্টিফিকেট প্রদান করে। একটি অনুমোদিত ডিজিটাল সার্টিফিকেটের সব অ্যাপ্লিকেশন এবং বৈধতা প্রত্যয়নের জন্য সিএরা দায়ী।

২৩. ডিজিটাল সার্টিফিকেট এর ব্যবহার কি হতে পারে?

উত্তরঃ ডিজিটাল সার্টিফিকেট দ্বারা ব্যবহারকারীর নাম এবং পাসওয়ার্ড ছাড়াই সয়ংক্রিয়ভাবে সদস্যপদ ভিত্তিক ওয়েব সাইট অ্যাক্সেস করার অনুমতি পাওয়া যায়। ই- মেইল বা অন্যান্য ইলেক্ট্রনিক নথির বিষয়বস্তু কোন উপায়ে ক্ষতিগ্রস্ত ছাড়াই প্রকৃত লেখক যার উদ্দেশ্যে প্রেরন করেছেন তিনি ডিজিটাল সার্টিফিকেট ব্যবহার করে তা যাচাই করতে পারেন। ডিজিটাল সার্টিফিকেটের মাধ্যমে কারও ব্যক্তিগত বার্তা পাঠানোর সময় অন্য কেউ এটা পড়তে সক্ষম হবে না।

২৪. ডিজিটাল সার্টিফিকেট ব্যবহার কতটা গুরুত্বপূর্ণ?

উত্তরঃ সামগ্রিক ইন্টারনেট নিরাপত্তা ব্যবস্থায় ডিজিটাল সার্টিফিকেট ও CA হল পিকেআই এর দু'টি উপাদান। পিকেআই সক্রিয় হলে যাদের একটি ডিজিটাল সার্টিফিকেট আছে তারা সবাই এটি ব্যবহার করতে বাধ্য হবে। এর ফলে, যারা ইন্টারনেট ব্যবহার করে ইলেকট্রনিক ব্যাংকিং, বাণিজ্য (তহবিল স্থানান্তর , ক্রয় এবং অন লাইন পরিশোধ), সরকারী সংস্থার সাথে অন

লাইনে লেনদেন (লাইসেন্স নবায়নের জন্য আবেদন, জরিমানা এবং বিল পরিশোধ), এবং ব্যবসায় অন লাইনে লেনদেন করে ডিজিটাল সার্টিফিকেট ব্যবহার ছাড়া তা একেবারে বন্ধ করে দেয়া হবে। সেইদিন খুব বেশী দূরে নয় এই লেনদেনের একমাত্র উপায় হবে ইন্টারনেট এবং ডিজিটাল সার্টিফিকেট সবার প্রয়োজনীয় অংশ হয়ে দাঁড়াবে।

২৫. কিভাবে ডিজিটাল স্বাক্ষর সার্টিফিকেট পেতে পারি?

উত্তরঃ সিসিএ অফিস শুধু সিএদের সার্টিফিকেট জারি করে। সিএরা সকল ব্যবহারকারীর জন্য ডিজিটাল স্বাক্ষর সার্টিফিকেট জারি করে থাকে। ডিজিটাল স্বাক্ষর সার্টিফিকেট পাওয়ার জন্য ছয়টি সিএ'র মধ্যে যে কোন একটি সিএ এর সাথে যোগাযোগ করতে হবে। নিম্নে ওয়েব সাইটের ঠিকানা গুলো দেওয়া হলোঃ

www.mango.com.bd

www.dohatec.com

www.data-edge.com

www.banglaphone.net.bd

www.computerservicesltd.com

www.bcc.gov.bd