

বাংলাদেশ ডিজিটাল স্বাক্ষর ও ডিজিটাল সনদ

১. পটভূমি

ভিশন ২০২১ বাস্তবায়ন অর্থাৎ ডিজিটাল বাংলাদেশ বিনির্মাণে সরকার আইসিটি সেক্টরে নানাবিধ পদক্ষেপ গ্রহণ করেছেন। এসব পদক্ষেপের মধ্যে অন্যতম হল দেশে পাবলিক কী ইনফ্রাস্ট্রাকচার (PKI) স্থাপন ও ডিজিটাল স্বাক্ষর প্রবর্তন করা। দেশে তথ্য ও যোগাযোগ প্রযুক্তির দ্রুত অগ্রগতির ফলে তথ্য ও যোগাযোগ প্রযুক্তির আইনগত বৈধতা ও নিরাপত্তা প্রদান করা সমীচীন ও প্রয়োজন। এ লক্ষ্যে সরকার ২০১১ সালের মে মাসে তথ্য ও যোগাযোগ প্রযুক্তি আইন, ২০০৬ (সংশোধিত ২০০৯, ২০১৩) এর আওতায় তথ্য ও যোগাযোগ প্রযুক্তি বিভাগের অধীন সংযুক্ত দপ্তর হিসেবে ইলেক্ট্রনিক স্বাক্ষর সার্টিফিকেট প্রদানকারী কর্তৃপক্ষের নিয়ন্ত্রক (সিসিএ) -এর কার্যালয় গঠন করে। এ সংস্থার প্রধান হলেন একজন নিয়ন্ত্রক যিনি সরকার কর্তৃক নিযুক্ত হন। সংস্থার প্রধান হিসাবে নিয়ন্ত্রক ইলেক্ট্রনিক স্বাক্ষর সার্টিফিকেট প্রদানকারী কর্তৃপক্ষের (সিএ) কার্যাবলী তত্ত্বাবধান ও নিয়ন্ত্রণ করেন এবং তাদের মধ্যে বিরোধ নিষ্পত্তিতে অগ্রণী ভূমিকা পালন করেন। তথ্য ও যোগাযোগ প্রযুক্তি আইন, ২০০৬ এর ধারা ৮ অনুযায়ী সকল সরকারী অফিসে ইলেক্ট্রনিক স্বাক্ষর ও ইলেক্ট্রনিক রেকর্ড ব্যবহারের স্বীকৃতি প্রদান করা হয়েছে।

২. ডিজিটাল স্বাক্ষর

ইলেক্ট্রনিক পদ্ধতির কার্যক্রমে নিরাপত্তা নিশ্চিতকরণে বিশ্বব্যাপী পরীক্ষিত ও স্বীকৃত প্রযুক্তি হল ডিজিটাল স্বাক্ষর। ডিজিটাল বাংলাদেশ বিনির্মাণের অংশ হিসেবে বর্তমানে দেশে ই-কমার্সসহ বিভিন্ন অনলাইন সেবা চালু করা হয়েছে। কিন্তু অনলাইন কার্যক্রমসমূহে ইলেক্ট্রনিক মাধ্যমে ব্যক্তির পরিচিতি ও তথ্যের নিরাপত্তা নিশ্চিত না করায় সাইবার আক্রমণের ঝুঁকি হ্রাস ও জালিয়াতি প্রতিরোধ করা দুরূহ হয়ে পড়েছে। এর ফলে তথ্য বিকৃতিসহ বড় ধরনের সাইবার অপরাধের মাধ্যমে জাতীয় পর্যায়ে অপূরণীয় ক্ষতির ঝুঁকি রয়েছে। ডিজিটাল/ইলেক্ট্রনিক স্বাক্ষর ব্যবহার করে তথ্যের অবিকৃত (Integrity) আদান-প্রদান, তথ্য প্রদানকারী ও গ্রহণকারীর পরিচিতি প্রতিপাদন (Authentication ও Non-Repudiation) এর পাশাপাশি তথ্যের গোপনীয়তা (Confidentiality) নিশ্চিত করা সম্ভব। এর ফলে জালিয়াতি প্রতিরোধ ও সাইবার অপরাধ হ্রাস করা যাবে। এ লক্ষ্যে উন্নত বিশ্বে ডিজিটাল/ইলেক্ট্রনিক স্বাক্ষর ব্যবহৃত হয়ে আসছে। ডিজিটাল/ইলেক্ট্রনিক স্বাক্ষর ব্যবহারের মাধ্যমে অনলাইন ট্রানজেকশনের নিরাপত্তা, নির্ভরযোগ্যতা ও বিশ্বাসযোগ্যতা নিশ্চিত করা সম্ভব হয়; অন্যথায় সাইবার নিরাপত্তার অভাবে ডিজিটাল কার্যক্রম বা ট্রানজেকশনসমূহ হুমকির মধ্যে পড়বে। তাই টেকসই ডিজিটাল উন্নয়নে সাইবার নিরাপত্তা নিশ্চিতকল্পে ডিজিটাল/ইলেক্ট্রনিক স্বাক্ষরের ব্যবহার অত্যাাবশ্যিক।

তথ্য ও যোগাযোগ প্রযুক্তি আইন ২০০৬ (সংশোধিত ২০০৯, ২০১৩) অনুযায়ী “ইলেক্ট্রনিক স্বাক্ষর” অর্থ ইলেক্ট্রনিক আকারে কোন উপাত্ত, যাহা-

ক) অন্য কোন ইলেক্ট্রনিক উপাত্তের সঙ্গে সরাসরি বা যৌক্তিকভাবে সংযুক্ত; এবং

খ) কোন ইলেক্ট্রনিক স্বাক্ষরের প্রমাণীকরণ নিম্নবর্ণিত শর্তাদি পূরণক্রমে সম্পন্ন হয়-

(অ) যাহা স্বাক্ষরদাতার সহিত অনন্যরূপে সংযুক্ত হয়;

(আ) যাহা স্বাক্ষরদাতাকে সনাক্তকরণে সক্ষম হয়;

(ই) স্বাক্ষরদাতার নিয়ন্ত্রণ বজায় থাকে এমন নিরাপদ পন্থায় যাহার সৃষ্টি হয়; এবং

(ঈ) সংযুক্ত উপাত্তের সহিত এটি এমনভাবে সম্পর্কিত যে পরবর্তীতে উক্ত উপাত্তের কোন পরিবর্তন সনাক্তকরণে সক্ষম হয়।

একই আইনে যে সকল ক্ষেত্রে স্বাক্ষরের বিষয় আছে সেগুলোর বেলায় ডিজিটাল স্বাক্ষরের বিষয়কেও সমবৈধতা দেয়া হয়েছে। যেমন-

- ইলেক্ট্রনিক রেকর্ড সত্যায়ন (ধারা -৫)
- ইলেক্ট্রনিক রেকর্ডের আইনানুগ স্বীকৃতি (ধারা -৬)
- ইলেক্ট্রনিক স্বাক্ষরের আইনানুগ স্বীকৃতি (ধারা -৭)

৩. ডিজিটাল সনদ

ডিজিটাল সনদ হল তথ্য বিনিময়ের ক্ষেত্রে দাতা কিংবা গ্রহীতা অথবা উভয় প্রান্তে ব্যবহৃত নিরাপত্তা নিশ্চিতকরণের একটি ইলেক্ট্রনিক প্রত্যয়ন ব্যবস্থা। একজন ব্যক্তি বা প্রতিষ্ঠান যখন অনলাইনে এমন কোন পরিষেবা গ্রহণ করে যেটি ডিজিটাল সার্টিফিকেট প্রদর্শন করে, তখন সে এই মর্মে আশ্বস্ত হয় যে, সেবাগ্রহণের কোন পর্যায়ে সেবাদাতা সংস্থার কোন ত্রুটির জন্য তার কোন তথ্য পাচার হয়ে যাবে না।

৪. সিকিউর সকেট লেয়ার (SSL) সার্টিফিকেট

এসএসএল সার্টিফিকেট হলো ডিজিটাল স্বাক্ষর সম্বলিত একটি আদর্শ নিরাপদ প্রযুক্তি, যা ওয়েব সার্ভার এবং ব্রাউজারের মধ্যে নিরাপদ এনক্রিপ্টেড সংযোগ স্থাপন করে। সাধারণত ওয়েব ব্রাউজার, সোশ্যাল মিডিয়া সাইট, ক্রেডিট কার্ড ট্রানজাকশন, ডাটা ট্রান্সফার এবং লগইন এর নিরাপত্তা বজায় রাখার জন্য এসএসএল সার্টিফিকেট ব্যবহৃত হয়।

৫. ডিজিটাল স্বাক্ষরের সুবিধাদি

- ডিজিটাল স্বাক্ষরের মাধ্যমে তথ্যের গোপনীয়তা (confidentiality), স্বাক্ষরকারী ব্যক্তি বা প্রতিষ্ঠানের পরিচিতি (authentication) ও তথ্যের অবিকৃতি (data integrity) নিশ্চিত কর যায়;
- ডিজিটাল স্বাক্ষর ব্যবহার করে বার্তা প্রেরণ করলে প্রেরক পরবর্তীতে সেটি অস্বীকার (non-repudiation) করতে পারে না;
- ডিজিটাল স্বাক্ষরকে হাতে লেখা স্বাক্ষরের সমান বৈধতা দেওয়া হয়েছে;
- ডিজিটাল স্বাক্ষরের আইনগত বৈধতা রয়েছে;
- ডিজিটাল স্বাক্ষর যাচাই করার সুযোগ রয়েছে;
- ডিজিটাল স্বাক্ষর একটি আন্তর্জাতিকভাবে স্বীকৃত পদ্ধতি;
- ডিজিটাল স্বাক্ষরের মাধ্যমে জালিয়াতি রোধ করা যায়;
- পেপারলেস অফিস সৃষ্টিতে ডিজিটাল স্বাক্ষরের প্রয়োজনীয়তা অনস্বীকার্য;
- ডিজিটাল স্বাক্ষর ব্যবহার করলে TCV (Time, Cost, Visit) যৌক্তিকভাবে কমিয়ে আনা সম্ভব;
- ডিজিটাল স্বাক্ষরের ব্যাপক প্রচলন গ্রীন ইকনমি নিশ্চিতকরণে ভূমিকা রাখে।

৬. ডিজিটাল স্বাক্ষর প্রবর্তনে গৃহীত পদক্ষেপ

৬.১ রুট সিএ এর PKI স্থাপন

- তথ্য ও যোগাযোগ প্রযুক্তি আইন, ২০০৬ (সংশোধিত ২০০৯, ২০১৩) এর আওতায় গঠিত ইলেক্ট্রনিক স্বাক্ষর সার্টিফিকেট প্রদানকারী কর্তৃপক্ষের নিয়ন্ত্রক (সিসিএ) - এর কার্যালয় রুট সিএ, বাংলাদেশ হিসাবে কাজ করে। সিসিএ কার্যালয়ে রুট সিএ এর পিকেআই স্থাপন করা হয়েছে। সর্বপ্রথম এপ্রিল, ২০১২ সালে সিসিএ'র রুট কী জেনারেশন কার্যক্রম সম্পন্ন করা হয়।
- ডিজিটাল স্বাক্ষর সার্টিফিকেট ব্যবস্থাপনা, অনুমোদন ও সংরক্ষণ করার জন্য প্রয়োজনীয় হার্ডওয়্যার, সফটওয়্যার, সংশ্লিষ্ট নীতিমালা, জনবল ইত্যাদির সমন্বিত সেটকে PKI (Public Key Infrastructure) বলা হয়।
- সিসিএ কার্যালয়ের রুট সিএ এর Hierarchical PKI মডেল –



৬.২ লাইসেন্স প্রদান

ডিজিটাল স্বাক্ষর প্রবর্তনের নিমিত্ত সিসিএ কর্তৃক ৬ (ছয়) টি প্রতিষ্ঠানকে সার্টিফাইং অথরিটি (সিএ) লাইসেন্স প্রদান করেছে।

1. Mango Teleservices Ltd.(<http://www.mangoca.com>)
2. Dohatec New Media (<http://dohatec-ca.com.bd>)
3. Data Edge Limited (<http://www.dataedgeid.com/>)
4. Bangla Phone Ltd. (<https://www.digitalsignature.com.bd/>)
5. Computer Services Ltd. (<https://ca.computerservicesltd.com/>)
6. Bangladesh Computer Council (<https://www.bcc-ca.gov.bd/>)

৬.৩ আইন, বিধি ও গাইডলাইন

- তথ্য প্রযুক্তি (সার্টিফিকেট প্রদানকারী কর্তৃপক্ষ) বিধিমালা, ২০১০
- বাংলাদেশ রুট সিএ সার্টিফিকেট অনুশীলন বিবৃতি, ২০২০ (CPS v 3.0)
- বাংলাদেশ রুট সিএ সার্টিফিকেট পলিসি, ২০২০ (CP v 1.0)
- টাইম স্ট্যাম্পিং সার্ভিসেস্ গাইডলাইন ফর সার্টিফাইং অথোরিটিজ, ২০১৬ (সংশোধিত ২০২০)
- ডিজিটাল স্বাক্ষর ইন্টারোপেরাবিলিটি নির্দেশিকা, ২০১৮ (সংশোধিত ২০২১)
- পিকেআই অডিট গাইডলাইন, ২০১৩ (সংশোধিত ২০২১)
- ই-সাইন সার্ভিস গাইডলাইন ফর সার্টিফাইং অথোরিটিজ, ২০২০

৬.৪ সচেতনতার সৃষ্টি ও প্রশিক্ষণ

- ডিজিটাল স্বাক্ষর ব্যবহার ও ক্ষেত্র সম্প্রসারণের জন্য সরকারী কর্মকর্তাদের ব্যবহারিক প্রশিক্ষণ প্রদান করা হচ্ছে;
- দেশব্যাপী ওয়ার্কশপ/সেমিনার আয়োজনের মাধ্যমে ডিজিটাল এবং সাইবার অপরাধ ও নিরাপত্তা সম্পর্কে জনসচেতনতা সৃষ্টির কার্যক্রম পরিচালনা করা হচ্ছে।

৭. ডিজিটাল স্বাক্ষর প্রাপ্তি ও ব্যবহার সংক্রান্ত তথ্য

সার্টিফিকেট প্রদানকারী কর্তৃপক্ষ (সিএ) গ্রাহক পর্যায়ে ডিজিটাল স্বাক্ষর সার্টিফিকেট ইস্যু করে। ডিজিটাল স্বাক্ষর সার্টিফিকেট সফট টোকেন, হার্ড/ক্রিপ্টো টোকেন এবং ব্যবহার বান্ধব ই-সাইন পদ্ধতিতে গ্রহণ করা যায়।

৭.১ ডিজিটাল স্বাক্ষর সার্টিফিকেট সংগ্রহ পদ্ধতি

হার্ড টোকেন এবং সফট টোকেনের মাধ্যমে অথবা ফাইল হিসাবে ডিজিটাল স্বাক্ষর সংগ্রহের পূর্বে নিম্নলিখিত পদক্ষেপ সম্পন্ন করতে হবে-

- প্রথমে ডিজিটাল স্বাক্ষর সার্টিফিকেট সংগ্রহ করার জন্য বৈধ সার্টিফিকেট প্রদানকারী কর্তৃপক্ষ (সিএ) এর সঙ্গে যোগাযোগ করতে হবে।
- এজন্য নির্ধারিত ফরম পূরণ করে সেটি সিএ'র নিকট জমা দিতে হবে। “কী-পেয়ার” (Key – Pair) তৈরি করার সময় একটি পাসওয়ার্ড/পাস-ফ্রেজ (Pass -Phrase) দিতে হবে যা একান্ত ব্যক্তিগত এবং গোপনীয়। সুতরাং তা যথাযথভাবে সংরক্ষণ করতে হবে।
- সিএ “কী” জেনারেট করার পর আপনাকে সার্টিফিকেটসহ সেটি হস্তান্তর করবে। আপনি ডাউনলোড করে সেটি ফাইল হিসাবে গ্রহণ করতে পারেন অথবা ক্রিপ্টো টোকেনের মধ্যেও সেটি গ্রহণ করতে পারেন। ফাইল হিসাবে গ্রহণের ক্ষেত্রে <Name>. p12 অথবা <Name>. pfx (ব্যবহারকারীর প্রাইভেট কীসহ সার্টিফিকেট) শীর্ষক একটি ফাইল পাবেন।

৭.২ হার্ড/ক্রিপ্টো টোকেন ব্যবহার পদ্ধতি

ডিজিটাল স্বাক্ষর প্রয়োগের ক্ষেত্রে হার্ড/ক্রিপ্টো টোকেন বহল প্রচলিত। টোকেনটি দেখতে ফ্ল্যাশ বা ইউএসবি (USB) ড্রাইভের মত, যা কম্পিউটার বা ল্যাপটপের USB পোর্টের সংযুক্ত করতে হয়। ফ্ল্যাশ বা ইউএসবি ড্রাইভের মত দেখতে হলেও এটি আপনার কম্পিউটারে কোন ড্রাইভ হিসাবে দেখাবে না। এটির ভিতরের কনটেন্ট দেখতে হলে ড্রাইভার সফটওয়্যার ইনস্টল করতে হবে। ড্রাইভারটি ইনস্টল করা হলে টোকেনটি initialize করতে হবে। টোকেন initialize করার সময় pin/password দিতে হবে। এই pin/password টি হল টোকেনটির নিরাপত্তার জন্য অর্থাৎ টোকেনটি হারিয়ে গেলেও কেউ এর কনটেন্ট ব্যবহার করতে পারবে না। initialize এর সময় পরপর কয়েকবার ভুল হলে হার্ড/ক্রিপ্টো টোকেনটি স্বয়ংক্রিয়ভাবে ব্যবহারের অনুপযুক্ত (disabled) হয়ে যাবে। টোকেনটি সবসময় নিরাপদ কোন স্থানে সংরক্ষণ করুন।

৭.৩ ই-সাইন পদ্ধতি

২০২১ সালে ডিজিটাল স্বাক্ষর সার্টিফিকেটের পাশাপাশি ব্যবহার বান্ধব ডিজিটাল ই-সাইন চালু করা হয়। বর্তমানে দুই ধরনের ই-সাইন সার্ভিস চালু রয়েছেঃ বেসিক এবং এডভান্স। বেসিক ই-সাইনের ক্ষেত্রে NID Verification এর মাধ্যমে গ্রাহকের e-KYC রেজিস্ট্রেশন সম্পন্ন করা হয়। এক্ষেত্রে ইস্যুকৃত ই-সাইনের মেয়াদ হয় সর্বোচ্চ ৩০ মিনিট। এডভান্স ই-সাইনের ক্ষেত্রে Biometric Verification এর মাধ্যমে গ্রাহকের e-KYC রেজিস্ট্রেশন সম্পন্ন করা হয়। এক্ষেত্রে ইস্যুকৃত ই-সাইনের মেয়াদ হয় ১-২ বছর। যেকোন ডকুমেন্টে ই-সাইন পদ্ধতিতে ডিজিটাল স্বাক্ষর প্রয়োগের পূর্বে two factor authentication এর মাধ্যমে স্বাক্ষরকারীর পরিচিতি নিশ্চিত করা হয়।