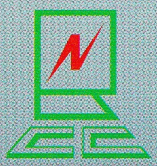
বাংলাদেশে ডিজিটাল স্বাক্ষর
ও
ডিজিটাল সনদ



বাংলাদেশ কম্পিউটার কাউন্সিল

বাংলাদেশে ডিজিটাল স্বাক্ষর ও ডিজিটাল সনদ

"আইসিটি এ্যাক্ট ২০০৬ বাস্তবায়ন এবং ই-কমার্স, ই-পেমেন্ট এবং ইলেক্ট্রনিক পদ্ধতিতে লেনদেনের জন্য অবকাঠামো সৃষ্টি করা।" **(কর্ম পরিকল্পনা-৪৮)**

"জনগণ এবং ব্যবসা-বাণিজ্যের জন্য প্রয়োজনীয় আন্তঃব্যাংক লেন-দেনের জন্য ইলেকট্রনিক পেমেন্ট গেটওয়ে স্থাপন করা।" **(কর্ম পরিকল্পনা-৮০)**

অনলাইনে লেনদেন করতে হলে দরকার এমন ব্যবস্থা যাতে অনলাইনে তথ্য প্রদানকারী, আবেদনকারী সবার পরিচয় 'প্রমাণযোগ্য' এবং নিশ্চিত হয়; একজনের সনাক্তকরণ চিহ্ন যাতে অন্যজন ব্যবহার করতে না পারে আর এতে যেন থাকে তথ্য/পরিচিতি যাতে হাতছাড়া না হয় তার নিশ্চয়তা। এসব কিছুর একটি সহজ সমাধান হলো ইলেকট্রনিক বা ডিজিটাল স্বাক্ষর ও ডিজিটাল সনদ।

ডিজিটাল স্বাক্ষর

ডিজিটাল স্বাক্ষর হল তথ্য বিনিময়ের ক্ষেত্রে তথ্য প্রদানকারীর পরিচয় যাচাইয়ের একটি (জটিল গাণিতিক) পদ্ধতি। এটি নিশ্চিত করে তথ্যটি যিনি পাঠিয়েছেন তার সেটি পাঠানোর কর্তৃত্ব আছে (তিনি নিজে) এবং যাত্রাপথে তথ্যটিতে কোন অনভিপ্রেত পরিবর্তন ঘটেনি। সাধারণত: ইন্টারনেট বা নেটওয়ার্ক আর্থিক লেনদেন বা অন্য কোন গোপনীয় লেনদেনের ক্ষেত্রে তথ্যের সঙ্গে ডিজিটাল স্বাক্ষর জুড়ে দেয়া হয়।

ডিজিটাল সনদ

ডিজিটাল সনদ হল তথ্য বিনিময়ের ক্ষেত্রে দাতা কিংবা গ্রহীতা অথবা উভয় প্রান্তে ব্যবহৃত নিরাপত্তা নিশ্চিতকরণের একটি ইলেকট্রনিক প্রত্যয়ন ব্যবস্থা। একজন ব্যক্তি বা প্রতিষ্ঠান যখন অনলাইনে এমন কোন পরিসেবা 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 যাবেনা।

ডিজিটাল স্বাক্ষর কীভাবে কাজ করে

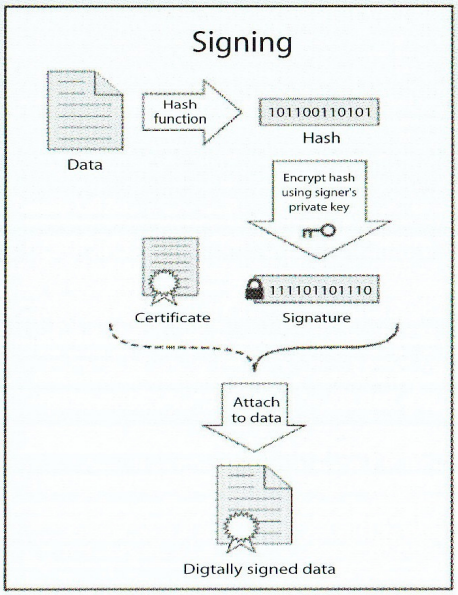
ডিজিটাল স্বাক্ষর ব্যবস্থার তিনটি অংশ।

১. একটি বিশেষ এলগরিদমের সাহায্যে একজোড়া (জটিল) গাণিতিক সংখ্যা তৈরি করা হয়। এই জোড়া সংখ্যা পরস্পর

এমনভাবে সম্পর্কযুক্ত যে, একটি থেকে অপরটি কখনো অনুমান/নির্ণয় করা যায় না, কিন্তু বিশেষ পদ্ধতিতে দুটো সংখ্যা আলাদাভাবে ব্যবহার করে একই ফল পাওয়া যায়। এই সংখ্যা দুটোকে বলা হয় কী বা চাবি (Key)।

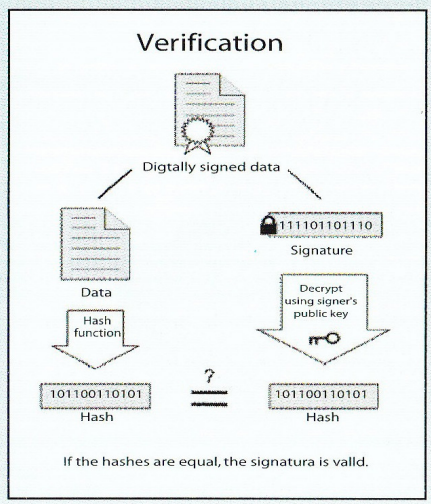
২. যে দলিলে স্বাক্ষর সংযুক্ত করা হবে সে দলিলকে একটি জটিল সংখ্যায় পরিণত করার পদ্ধতি যা ঐ দলিলের জন্য অনন্য। এই জটিল রূপান্তরের জন্য একটি বিশেষ পদ্ধতি ব্যবহার কর হয়। একটি বিশেষ গাণিতিক রাশিমালা ব্যবহার করে এই গাণিতিক সংখ্যাটি পাওয়া যায়। যার মাধ্যমে এটি করা হয় সেটিকে বলা হয় হ্যাশ (Hash) ফাংশন আর সংখ্যাটিকে হ্যাশ। এটি একটি একমূখী পরিবর্তন ব্যবস্থা। অর্থাৎ এর মাধ্যমে দলিল থেকে হ্যাশ পাওয়া যাবে কিন্তু হ্যাশ থেকে দলিলকে উদ্ধার করা যাবে না।

৩. হ্যাশ এবং কী-এর সমন্বয়ে তৈরি হয় ডিজিটাল স্বাক্ষর ও প্রমাণীকরণ ব্যবস্থা।



জটিল গাণিতিক সংখ্যা বা চাবি দুটোর একটি হলো নিজের জন্য গোপনীয় চাবি (Private Key) এবং অন্যটি হলো সবার জন্য উন্মোচনের চাবি (Public Key)। প্রেরক যে দলিল পাঠাবেন প্রথমে নির্দিষ্ট নিয়মে সেটিতে হ্যাশ ফাংশন প্রয়োগ করেন। এর মাধ্যমে দলিলের একটি হ্যাশ তৈরি হয়। তারপর তার Private Key দিয়ে সেই হ্যাশটিকে একটি 'একক' চিহ্নে [ডাইজেস্ট বা ডিজিটাল স্বাক্ষর]

পরিণত করেন। কম্পিউটার প্রোগ্রাম দিয়ে এটি করা হয়। তারপর দলিল ও স্বাক্ষর দুটোই প্রাপকের কাছে পাঠিয়ে দেন।



প্রাপক প্রথমে একই নিয়মে প্রাপ্ত দলিলকে হ্যাশে পরিণত করেন। প্রাপক প্রেরকের Public Key যোগাড় করে নেন। আর প্রেরকের Public Key দিয়ে স্বাক্ষর থেকেও হ্যাশ বের করেন। দুটো হ্যাশ এক হলে সনাক্তকরণ নিশ্চিত হয়।

এ পদ্ধতির বিশেষত্ব হলো এতে কোন শারীরিক বা মানসিক শক্তির প্রয়োগ নেই। এতে একটি নির্দিষ্ট নিয়মে, standard software ব্যবহার করতে হয়। প্রেরিত দলিলভেদে স্বাক্ষর হয় ভিন্ন। ফলে নকলের কোন সুযোগ নেই। এটি একটি অনন্য বৈশিষ্ট্য। কোন ব্যক্তির দুটো চিঠির জন্য তার ডিজিটাল স্বাক্ষর হবে দুটো। প্রেরকের পরিচয় যাচাই -এর কাজটিও হয় কম্পিউটার প্রোগ্রামের মাধ্যমে। যে সকল এলগরিদম ব্যবহার করা হয় সেগুলো নির্দিষ্ট ও মানভিত্তিক।

বাংলাদেশে ডিজিটাল স্বাক্ষর ব্যবস্থা

আমাদের তথ্য এবং যোগাযোগ প্রযুক্তি আইন ২০০৯-এ "ইলেকট্রনিক স্বাক্ষর":

"ইলেকট্রনিক স্বাক্ষর" অর্থ ইলেকট্রনিক আকারে কোন উপাত্ত যাহাঃ-

ক) অন্য কোন ইলেকট্রনিক উপাত্তের সঙ্গে সরাসরি বা যৌক্তিকভাবে সংযুক্ত এবং

খ) কোন ইলেকট্রনিক স্বাক্ষরের প্রমাণীকরণ নিম্নবর্ণিত শর্তাদি পূরণক্রমে সম্পন্ন হয়ঃ-

(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 এমনভাবে সম্পর্কিত যে পরবর্তীতে উক্ত উপাত্তে কোন পরিবর্তন সনাক্তকরণে সক্ষম হয়।

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

- ইলেক্ট্রনিক সত্যায়ন বৈধ (ধারা-৫(১))
- প্রযুক্তি নিরপেক্ষ পদ্ধতি বা স্বীকৃত পদ্ধতির ব্যবহার (ধারা-৫(২))
- ইলেক্ট্রনিক রেকর্ডের অভিগম্যতা থাকলে সেটি স্বীকৃত দলিল (ধারা-৬)
- ইলেক্ট্রনিক স্বাক্ষর আইনানুগভাবে স্বীকৃত (ধারা-৭)

ডিজিটাল স্বাক্ষর চালু হলে কী লাভ হবে

- বাংলাদেশে ই-কমার্স চালু হবার ক্ষেত্রে একটি বড় বাধা অপসারিত হবে;
- অনলাইনে নানা রকমের লেনদেন করা যাবে;
- অনলাইনে কেনা-কাটা করা হবে। টেন্ডারবাজি বন্ধ হবে;
- কর দেয়া সহজ হবে, ফলে করদাতার সংখ্যা বেড়ে যাবে;
- দরখাস্ত জমা দেয়ার জন্য সশরীরে অফিসে হাজির হতে হবে না;
- সরকারের সঙ্গে অনেক লেনদেন দেশের যে কোন স্থান থেকে করা যাবে;
- অনেক পুরোনো আর্কাইভ থেকেও চোখের পলকে তথ্য বের করা যাবে;
- একাধিক দপ্তর একই তথ্যভান্ডার ব্যবহার করলে আন্তঃমন্ত্রণালয় তথ্য বিনিময় ও কার্যপদ্ধতি সুসংহত হবে;
- দাপ্তরিক পর্যায়ে কাগজের ব্যবহার হ্রাস পাবে, নথিতে নোট লিখে সেটি সই করার পরিবর্তে ই-ফাইলে কাজ করা যাবে;

- যেহেতু ডিজিটাল সনদ ও ডিজিটাল স্বাক্ষর ব্যতীত টাকা-পয়সা অনলাইনে বিনিময় হবে না, কাজেই সরকারের অগোচরে বেআইনী কোন খাতে (যেমনঃ জঙ্গীবাদ, হুন্ডি বা মুদ্রাপাচারে) টাকা-পয়সা ব্যবহৃত হবার সুযোগ থাকবে না;
- সরকারী তথ্যসমূহ অনলাইনে বিনিময়ের ক্ষেত্রে ফাঁস হবার কোন সুযোগ থাকবে না;
- তথ্য বিনিময়ের সকল পর্যায়ে স্ট্যাটাস ট্র্যাক করা যাবে, যেটি যে কোন সংঘটিত সাইবার অপরাধের তদন্তে কাজে দিবে।

বাংলাদেশ কম্পিউটার কাউন্সিল

আগারগাঁও, শেরে বাংলা নগর, ঢাকা-১২০৭

ফোনঃ +৮৮০-২-৮১৪৪০৪৬, ফ্যাক্সঃ +৮৮০-২-৯১২৪৬২৬

ই-মেইলঃ bcc@bcc.n-et.bd ওয়েবঃ www.bcc.net.bd