Digital signatures not catching on

By *Pavan Duggal*, | 18 Jul, 2004, 12.16AM IST Post a Comment

The Information Technology Act 2000 provides for the legal authentication of electronic records by means of digital signatures.

It stipulates that the authentication of the electronic record is to be effected by the use of the asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

The law further explains that the "hash function" is an algorithm mapping that translates one sequence of bits into another, generally smaller set, known as "hash result".

An electronic record yields the same hash result every time the algorithm is executed. It makes it computationally infeasible to derive or reconstruct the original electronic record from the hash result produced by the algorithm. Secondly, two electronic records will not produce the same hash result using the algorithm.

The Indian Cyberlaw doesn't just provide for the legal recognition of digital signatures. It also states that "where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of digital signature affixed in such manner as may be prescribed by the Central Government".

The law also provides for various provisions relating to secure digital signatures. The law stipulates that if, "by application of a security procedure agreed to by the parties concerned, it can be verified that a digital signature, at the time it was affixed, was—(a) unique to the subscriber affixing it; (b) capable of identifying such subscriber; (c) created in a manner or using a means under the exclusive control of the subscriber and is linked to the electronic record to which it relates in such a manner that if the electronic record was altered the digital signature would be invalidated, then such digital signature shall be deemed to be a secure digital signature".

The Indian Cyberlaw has also provided for a detailed digital signature regime and its regulation. The Controller of Certifying Authorities is the relevant statutory authority, which has been given the power to control and exercise superintendence over the functioning of certifying authorities and their licencing-related issues.

Certifying authorities are legal entities which are responsible for issuing digital signatures

certificates to citizens. The law has not only defined the responsibility but also the duties and functions of licensed Certifying Authorities and subscribers of digital signature certificates.

The law also requires that every subscriber will exercise care to retain control of the private key corresponding to the public key listed in his Digital Signature Certificate and take all steps to prevent its disclosure to a person not authorized to affix the digital signature of the subscriber.

With the digital signature regime in the country already set up, the Controller of Certifying Authorities has already issued licences to numerous legal entities to operate as certifying authorities.

However, we have not seen a massive adoption of digital signatures in our country by end users or the market. There seems to be lack of awareness about digital signature certificates and their adoption and usage. It is, however, expected that digital signature certificates will occupy a major role in driving the growth of the e-economy of India.

Our company provides free web based email service to people in the community. Our technical engineers handle the service and I run the entire show. I have just found that one of the engineers had, without permission of email subscribers, placed a software in our systems which enabled him to retain a copy of the emails. I terminated the services of the engineer as soon as I came to know about this. Are there any legal ramifications to this issue?

You have raised a significant issue regarding the right to privacy of email subscribers and the liability of email service providers. Netizens today are putting up a strong fight to preserve their privacy. There are various privacy battles that have been fought on the internet. However, the question that arises is whether you, as an email service provider, can actually peep through and see/ read the email of your subscribers. The law is not fully crystallized on this issue.

However, under the Indian Cyberlaw, you are a network Service Provider and you are liable for any third party data or information made available by you. So if your employee has actually gone ahead and read the email of your clients without their permission, it is a violation of the Indian cyberlaw and you have opened yourself to both civil and criminal liability.

The civil liability can actually mean damages by way of compensation to the tune of Rs 1 crore. Criminally, you can be liable for imprisonment for a couple of years. It is interesting to note however, that such a case has not been tested in the Indian courts.

However in a recent case in the United States, a court came across findings that surprised the world. An action was bought by a subscriber against the service provider as it had installed a software which enabled it to read the contents of subscribers' emails.

The US court held that the email service provider was not liable for the act of reading the subscriber's email. It stated that email service providers have the right to monitor, read, and take copies of any emails pertaining to any subscriber to those services.

In a 2 to 1 majority decision, the Massachusetts Appeal Court observed that email does not enjoy the same legal protection from interference as snail mail services and telephone calls.

The court ruled that because email is stored, even if for some nanoseconds, on an ISP's servers before being routed to its recipient, it is not subject to the same legal safeguards


annum: World Bank


A bank is known by the network it keeps, literally!


50% smallcap stocks at risk if earnings fail to catch up


Best localities in Noida to buy a home!

Sponsored by Prop Tiger


Mahindra set to launch its smallest offering 'Mahindra KUV100'


6 BYOD Oversights Enterprises Must Avoid


Gesture grey analog men's watch @ Rs.335

Sponsored by Indiatimes Shopping


Start up India: Silicon Valley CEOs eyeing goodies like tax exemptions on capital gains

RBI Governor Raghuram Rajan will meet bank chiefs next week to review state of bad loans


Look into the cloud before you leap

Poll

Will India benefit significantly from falling commodity prices?

- Yes
- No
- Can't say

VOTE

Open a free online trading a/c. Now is the right time!

Sponsored by Sharekhan

Indian Railways gets first model rake of luxury

that apply to the bugging of phone calls or the opening of documents in transit in the US Post office mail system.

The court said that email service providers are entitled to intercept and open email because they store the communications. However, the dissenting judge, in the 2 to 1 ruling, Kermit Lipez said the decision would have far-reaching effects on the personal privacy and security of electronic communications.

This is a very strange judgement and is likely to further complicate the scenario relating to the liability of network service providers. It will be interesting to see the development in this regard. Meanwhile, I would suggest that safety is the best form of caution and that you need to take all steps to legally protect yourself.

'Make in India' coaches

Ram Jethmalani withdrew offer to defend Sonia, Rahul Gandhi after Parliament disruption

6 Essentials to Look for in Your Collaboration Service Provider

As clock ticks down on sanctions, oil-laden Iran tankers set to target India and Europe

Crude oil at $30 may not be good news for you; here's why

Pathankot attack: Follow Israel's top-notch technology tricks to protect India-Pakistan border

9 hot budget smartphones coming to India in 2016

India has huge opportunity for app driven economy in consumer space

Defence Ministry's Rs 13,500 crore warship order will throw up a major opportunity for private sector

Controversy over depiction of Lord Jagannath delays issue of commemorative coins on occasion of Nabakalebara

M&M launches compact SUV KUV100 at a starting price of Rs 4.42 lakh