ODYSSEY
cryptic by intent

EVIDENTIARY VALUE OF PUBLIC KEY TECHNOLOGY AND PUBLIC KEY BASED SIGNATURES

ODYSSEY TECHNOLOGIES LTD.

EVIDENTIARY VALUE OF PUBLIC KEY TECHNOLOGY AND PUBLIC KEY BASED SIGNATURES

Public Key Cryptosystems are used to create non-repudiation on digital selections. As digital information is infinitely copyable and changeable, the various technologies used for persistent user authentication fall short one way or other. Most of the shortcomings stem from the fact that all of them use a form of a shared secret and the user will always be able to prove that such authentication could have been created by at least one other person. Such systems in usage include passwords, one time passwords, swiping of a magnetic card, a finger print etc.

Public Key Systems rely on the fact that only the user creates, stores and eventually destroys some information (the private key) which is never shared with anyone else. The user computes the signtature using the private key and such key is verifiable by anyone who possesses the corresponding public key. As the public key itself cannot be used for creating the signature, it results in a persistent record which can be used to prove the user action any time later.

Passwords

Passwords are usually simple secrets chosen by the user which are then shared with the service provider and registered as the user's password. In the early days, passwords were exchanged in plain text and were stored as such by the service provider in his system. Thereafter, every time the user needed to access resources or carry out transactions on the service provider's system, he tendered the password again and the system compared it with the stored password.

The system has since been improved by sending passwords through encrypted channels or sending a hash or other modified form of the password rather than as entered by the user. More sophisticated systems do not use the password directly but use it to encrypt some known value (like the current date, or a random value sent by the server) in the client side and decrypt the same on the server side to authenticate the user. These improvements make it more difficult for a man in the middle to recover the password or to replay earlier user-actions.

Nevertheless, the essence of the passwords remain the same. There is a secret that is shared between the user and the service provider. Either side can carry out the same action.

Systems which use passwords for transaction authentication can run into this problem any time a user wants to repudiate his transaction. He can claim that someone on the service provider's side could have used the password (or its derivative) to create the same evidence. Even though the service provider can claim that his systems have sufficient safeguards against such insider-activity, it would not be possible to conclusively prove that only the user carried out the action.

Therefore, the evidence of password based transactions entirely rests on the service provider's logs. In any dispute, as it is an internal record entirely in the control of the service provider, the evidentiary value will be minimal.

A physical equivalent of the passwords will be an account holder walking into a bank and the teller handing him money after asking the user for his password without any cheque or withdrawal form. Even in the world of perfect tellers who faithfully record every customer's password in a logbook, such a system will not carry sufficient evidentiary value.

One Time Password

One time passwords are passwords that change for every use. In their ideal form, a starting value (seed) is chosen by the user and using a software, the seed is hashed (using MD5 or some such algorithm) a large number of times. The resulting digest is registered with the service provider.

The next time the user wants to be authenticated, he takes the seed again and hashes it for one less than the original hash count. Thus, if originally the seed was hashed 10000 times, the second time he hashes it 9999 times. The service provider receives the digest and hashes it one more time making it 10000 times again. This value will be compared with the original registered value and if it matches, authentication will be successful.

The next time, the user will hash the seed for 9998 times and send the digest. The bank will digest it once more and compare with the previously stored 9999 digest, and so on. Once the hash count comes down near 1, the sequence will be reinitialized.

This is a perfect form for authentication but still not good enough for transactions. As the digest sequence will be revealed to the service provider one after the other, eventually all the secrets are shared between the user and the service provider. The same issue as with the passwords exists here also.

In practice, as it would be difficult for the user to enter a 16 byte digest (32 hex digits), a even weaker system is followed. In real OTP systems, the digesting is carried out more as a randomizing method than a one-way function. Instead, a random number generated by using the current time or some such value along with a shared key value and digesting it a given number of times. This does not even leave a temporary unshared secret in the hands of the user as the canonical OTP scheme described above.

Magnetic cards, other storage cards, and biometrics

Though it is strange to combine these three under one heading, in theory all the three are the same. A relatively unique secret data is stored in a magnetic card or other memory card and is automatically read by a device during authentication. In the case of biometrics, the naturally stored data of the user's biometrics (fingerprint, retinal pattern or whatever else) is read by the system and communicated to the service provider.

These systems are good enough for supervised authentication, like a user gaining entry to a premise where a security guard watches to see that the user does not tamper with the mechanism. However, the same does not hold true in the Internet where data injection is easy to achieve. Thus A can obtain B's fingerprint in some way and inject it into the transaction stream to authenticate B; and the back end system, in most cases can be effectively fooled.

Even where the biometrics or other data is used in a fool-proof manner, they will still not serve the purpose of non-repudiation as there is no persistent data that only the user could have created. If anything, the evidentiary value for non-repudiation is weaker than those of passwords and one time passwords.

Public Key based systems

The Public Key Based systems work by using dual keys. A private key, that is in the exclusive possession of the user and a public key that is distributed to anyone and at a minimum shared with the service provider.

The private key is capable of encrypting data submitted to it which can be decrypted only by its related public key. When such encryption is carried out on a hash of some data, it is called a digital signature.

In the current state of technology, RSA public key systems provide, at an appropriate key size, signatures that cannot be reverse engineered within any meaningful time. For a normal attacker, this can translate to hundreds of years of effort.

Since the signature can be created only by the person holding the private key, the public key signature systems are recognized to be the only model for ensuring non-repudiation of transactions.

Even the Public Key systems need certain safeguards to derive maximum evidentiary value from the signatures. The first is that the user should create and manage his private key at all times. The second is that the public key should be securely obtained and stored by the service provider. In practice, it is usually done by embedding the public key and the user attributes in a digital certificate and a certifying authority signing the certificate.

Thus in systems where the key pair is securely generated by the user, and a digital signature is obtained from the user using his private key, the signature carries a very high evidentiary value.

Information Technology Act provides for the use of this technology for creating digital signatures. It additionally provides for licensing of certifying authorities who can identify the subscribers and certify their public key. Such certificates are also accorded a higher status under the Information Technology Act as well as the amendments to the Evidence Act, Negotiable Instruments Act etc.,

The status accorded by these statutes state that any signature created using a licensed CA certificate will automatically be accepted as evidence. This is done by sections 85B and 85C of the Evidence Act which create a presumption that a digitally signed record has not been tampered with. Section 85C creates another presumption that once a certificate is accepted by the subscriber, the data on the certificate will be presumed correct.

Further, sections 67 and 67A of the Evidence Act, describe the situation more clearly.

The Indian Evidence Act, 1872 :

67. Proof of signature and handwriting of person alleged to have signed or written document produced

If a document is alleged to be signed or to have been written wholly or in part by any person, the signature or the handwriting of so much of the document as is alleged to be in that person's handwriting must be proved to be in his hand writing.[1]

67A. Proof as to electronic signature

Except in the case of a secure electronic signature, if the electronic signature of any subscriber is alleged to have been affixed to an electronic record the fact that such electronic signature is the electronic signature of the subscriber must be proved.[2]

Every signature needs proof. What the amendment to the Evidence Act has done is to shift the burden of such proof in cases of secure digital signatures. It must be noted that even in the case of licensed CA issued certificates, not all digital signatures will be considered 'Secure Digital signature'

The Indian I.T Act, 2000

15. Secure electronic signature.

An electronic signature shall be deemed to be a secure electronic signature if-

- *the signature creation data, at the time of affixing signature, was under the exclusive control of the signatory and no other person; and*
- *the signature creation data was stored and affixed in such exclusive manner as may be prescribed.*

Explanation:
In case of digital signature, the 'signature creation data' means the private key of the subscriber.[3]

Whereas, the definition of digital signature in the I.T.Act is given as below:

(p) "digital signature" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3;[4]

[1] Chapter V, 67, The Indian Evidence Act, 1872

[2] The Second Schedule: Amendments To The Indian Evidence Act, 1872

[3] Chapter 5, Section 15, Amendment to the Indian IT Act 2008

[4] Chapter 1, Section 2, The Indian IT Act 2000

3. Authentication of electronic records.

1. *Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his digital signature.*

2. *The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.*

Explanation:

For the purposes of this sub-section, "hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as "hash result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible—

(a) *to derive or reconstruct the original electronic record from the hash result produced by the algorithm;*

(b) *that two electronic records can produce the same hash result using the algorithm.*

3. *Any person by the use of a public key of the subscriber can verify the electronic record.*

4. *The private key and the public key are unique to the subscriber and constitute a functioning key pair.*[5]

Thus, the I.T.Act itself makes a distinction between 'digital signatures' and 'secure digital signatures' and it is only the 'secure digital signatures' which are accorded a special status in the Evidence Act. Section 85B of the Evidence Act clarifies the situation further by clearly stating that the presumption of proof is only available for secure digital signatures.

85B. PRESUMPTION AS TO ELECTRONIC RECORD AND DIGITAL SIGNATURES

1. *In any proceedings involving a secure electronic record, the Court shall presume unless contrary is proved, that the secure electronic record has not been altered since the point of time to which the secure status relates.*

2. *In any proceedings, involving secure electronic signature, the Court shall presume unless the contrary is proved that-*

(a) *the secure electronic signature is affixed by subscriber with the intention of signing or approving the electronic record;*

(b) *except in the case of a secure electronic record or a secure electronic signature, nothing in the section shall create any presumption relating to authenticity and integrity of the electronic record or any electronic signature.*[6]

This does not mean that normal digital signatures do not carry any evidentiary value. On the contrary, the other digital signatures will be under the purview of the second part of section 67A *"that such electronic signature is the electronic signature of the subscriber must be proved"*

Thus in all the cases of digital signatures except secure digital signatures, that the signature was created by the subscriber is to be

[5] Chapter 2, Section 3, The Indian IT Act 2000

[6] Section 85B, The Evidence Act

proved. This is the same as the stipulation in Section 67 which states that the signature must be proved in the case of physical documents.

It should also be remembered that there is nothing in the law that prohibits the use of PKI without using a certificate issued by the certifying authority. It is simply that no special recognition is accorded to non-licensed CA certificates and with reference to proof.

As PKI is the stipulated technology under the Information Technology Act, even in non-licensed CA certificate cases, the signatures can be proved by the strength of the technology whereas, in the case of any other technology, the signatures cannot be proved.

To further illustrate the point, we can consider a signature created from a licensed CA as a notarized signature. In the other cases, it can be considered to be a normal signature which we use in our everyday lives. Both are valid and are provable but the notarized signature is prima facie considered valid.

To put the different models in perspective, they are compared in the table below with reference to the various attributes.

Attribute	Licensed CA Issued Certificates	Own CA Issued Certificates	Passwords, One Time Passwords
Signature Status under evidence Act	If it is a 'secure digital signature' the authenticity is presumed and need not be proved. If it is other signature, it must be proved but the proof will be simple.	It must be proved but the proof will be simple with a user agreement.	It must be proved but the proof will be impossible.
Under I.T.Act	Signature presumed to be that of the subscriber.	Signature can be proved to be that of the user with proper registration process.	It must be proved but the proof will be impossible.Technology not mentioned in the Act.
Operation - Issuance	The certificates must be issued as a sub-CA of a licensed CA. The registration can be complex.	The registration will be moderately complex.	For passwords, registration is very simple. For biometrics, the re-registration can be complex.

Operation - Usage	Every time a signature is created, revocation status is to be checked from the CA. No CA offers provision for revocation cycles of less than one day.	The revocation is instantaneous and the validation checks will be entirely inside the network and instantaneous.	There is no separate revocation process. The user changes his password at will.
Operation - Latency	The latency of each transaction can be very high.	Very little additional latency to the normal transaction times.	Very little additional latency.
Cost	The recurring cost of the certificates is very high. There is the additional cost of deploying a gateway application like Snorkel.	There will be no recurring cost other than AMC for the software.	For passwords, no recurring cost. For OTP, the devices have to be replaced periodically at a high cost. For biometrics, the users should invest in additional hardware.
Operational Dependency	Will be dependent on CA's CRL system. Downtimes of CRL will cause the web application to be stopped.	No external dependency.	No external dependency
Customer Ease	The registration process will be complex. As the certificates can be used for multiple purposes, a private key loss can have high cost in money and time.	As simple to use as passwords.	Simple to use.

About Odyssey

Odyssey Technologies Limited is a pioneer in PKI technology in the Asia-Pacific region. The company develops products and solutions for transaction security and is recognized by the Controller of Certifications in India as a technology vendor.

By isolating the security components and business logic, Odyssey stays true to its zero-touch philosophy and ensures deployment of solutions quickly and effectively without the need for integration or changes to the existing code-base. The company proudly supports the security needs of major banks and financial institutions in the Asia-Pacific region and has earned their trust as a reliable vendor.

Odyssey Technologies Limited is based in Chennai, India and is listed in the Bombay Stock Exchange.

To learn more about solutions from Odyssey Technologies Limited, visit www.odysseytec.com or e-mail info@odysseytec.com.

ODYSSEY
cryptic by intent

ODYSSEY TECHNOLOGIES LTD.