ISSN 2229-5518

# Digital Signature on-line, One Time Private Key [OTPK]

## online certification process with strong (2-factor) authentication

Vinod Moreshwar Vaze

***Abstract* —** Downsizing of computers & requirement of higher security has shifted the demand for enhanced security solutions. Need of the hour is to have a security system which is doubly safe, and yet suitable for "hand held devices". One Time Private Key (OTPK) allows the users to generate their signing keys and use their strong authentication to certify the signing keys and sign the transaction/document, hereafter the signing keys will be erased.

**Keywords –** Digital Signature, Public Key Infrastructure (PKI), Asymmetric encryption, Private Key, Public Key, Strong Authentication

## 1. Introduction (Digital Certificate)

As a part of e-governance initiative, the income tax department, Ministry of Finance, Govt. of India encourages tax paper to e-file their returns. It is mandatory for companies and firms requiring statutory audit u/s 44AB to submit income tax return electronically. In order to participate in E-Tendering, E-Procurement of Orders, etc. Very soon, not only every director / signing authority but also everyone, you and me, as a good taxpaying citizen of India, would be required to have a Digital Certificates.

There is no doubt that the demand for "Digital Signature" is going to increase many times. Now the question is "would the demand for Digital signature operated from a mobile phone would gallop or people would still be using a computer (lap-top)?

## 2. The Concept of Digital Signature

How do I digitally Sign a document? What happens at the back-end? Explained in simple terms.

Take the following steps to digitally sign a document.

1. First take a Message Digest, here-in-after referred as: hash (#) using any standard Message Digest Algorithm such as MD5. (This can easily be download from the Internet, free of cost) of the softcopy of the document to be signed.
2. Now encrypt this hash (#) with your Private Key.
3. This process returns your Digital Signature.
4. Corollary: If one Decrypts the Digital signature with your public key it returns back the hash (#)

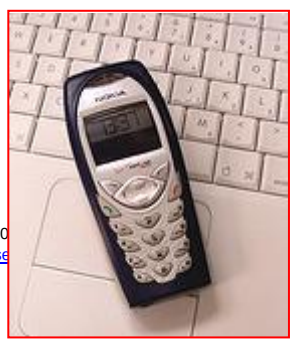
## 3. The Modus Operandi of Digital Signature

### 3.1. The practical use of Digital Signature:

***Sender's side:*** Take Hash of which ever document you need to send securely.
2. Get Digital Signature by Encrypting the Hash with senders Private Key.
3. Concatenate the document with the digital Signature.
4. Encrypt them together by a Symmetric key.
5. Also Encrypt the Symmetric with receiver's public key.
6. Get the digital envelope. Send this to the receiver.

***Receiver's side***
6) Receive the digital envelop.
7) Decrypt the "encrypted Symmetric key" with receivers Private key.
8) Get the symmetric key.
9) Decrypt the "encrypted & signed" document with this freshly obtained symmetric key.
10) Separate the Digital signature
11) Decrypt the digital signature with sender's public key and get Hash (say #1). The document can be hashed by the same standard Message Digest Algorithm the sender has used (say MD5). Get Hash (say #2). Now compare #1 with #2.
Is it the same? Yes then we achieve Integrity, Authenticity, Privacy, Secrecy, Non repudiation and replay protection. Digital Signature has come a long way now.

### 3.2. Cell phone penetration in India.



Today 70% of Indian population has a mobile phone. Noting the fact that the number of cell-phone subscribers will soon exceed the population of India, one can


- *Vinod Moreshwar Vaze*
- *B.Tech. (I.I.T., Kanpur) PGDFM, Diploma in Cyber Law, Internet Security Professional*
- *Research Scholar, JJT University, Rajasthan*
- *Centre for Excellence in Education, 301, Sachinam Almeida Road, Thane 400602*
- *vinod_vaze@hotmail.com*

easily conclude what the society would demand in near future.

From convenience point of view the people on the move would be happy to use a cell to digitally sign any document rather than a laptop/ PC. No doubt about that. The central theme of this paper is to find if from security point of view would the people have faith in a hand held device?

The general trend now-a-days is to use:

1. A Hand held device. (smaller the better)
2. On-Line transaction from your cell phone.
3. Work with devices lower power consumption.
4. Work with devices having lower overheads.
5. More and more businesses are moving to the on-line media for transactions and payments.

Thus the need for the hour is to have:

1. A technology which is easier to use to get digital signature.
2. A device which is cheaper. (Both the initial cost and the running cost)
3. A system which is faster to adopt for a common man.
4. A digital certificate which can be operated from your mobile phone.
5. A technology which offers Strong Authentication (something more than just one layer)

**Challenge:**

Laws surrounding the use of digital signatures are becoming stricter, making security for mobile users challenging. In many Asian and European countries, such as Singapore and Germany, government's mandate that private keys used for digital signatures must be in possession of the user at all times. According to Tan Teik Guan, CEO and CTO (Chief Technical Officer) of Data Security Solutions, this rules out most of the technology available to mobile users today.

**Solution:**

Guan and his team are developing an OTPK, or one-time private key, to enable mobile and other users to digitally sign electronic transactions and documents.

1. With OTPK, a key is generated via a browser-based Java applet whenever a user needs to carry out a signature on a device or browser.
2. That key is sent for certification, used to sign the transaction or document, and then deleted.
3. Though the key is no longer available, the certification chain remains so users are able to revalidate their documents.
4. OTPK uses strong cryptography, including RSA 1024 (Ron Rivest, Adi Shamir and Leonard Adleman) for PCs and ECDA for mobile phones, to ensure the highest level of compliance and privacy.
5. Guan says OTPK will enable tightened security for mobile applications such as allowing doctors to digitally sign prescriptions from their mobile phones

PKI ( public key infrastructure)

Request for Comment RFC 2822 (Internet Security Glossary) defines public-key infrastructure (PKI) as the set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates based on asymmetric cryptography.

The principal objective for developing a PKI is to enable secure, convenient, and efficient acquisition of public keys. The Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (PKIX) working group has been the driving force behind setting up a formal (and generic) model based on X.509 that is suitable for deploying a certificate-based architecture on the Internet.

### 3.3. X.509 standards

X.509 is an ITU-T (International Telecommunication Union) standard for a public key infrastructure (PKI)

**The traditional PKI.**

1. Application server send the document to be signed to the client server (user) for Digital Signature
2. The user inserts the card/ token/ pen drive / perform the biometrics as given & instructed by Certificate Authority (C.A. ) / or Registration Authority (R.A.)
3. The user follows the instructions given by C.A./ R.A and the Digital Signature is created.
4. This digital signature is then send to the "time-stamp" server for stamping date, time etc.
5. Application server, from time to time, uses OCSP protocol for look-up and follows up.

**OCSP**

OCSP (Online Certificate Status Protocol) is a common scheme for maintaining the security of a server and other network resources. The Online Certificate Status Protocol (OCSP) is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate.

It is described in RFC 2560 (request for comment) and is on the Internet standards track. It was created as an alternative to Certificate Revocation Lists (CRL), specifically addressing certain problems associated with using CRLs in a Public Key Infrastructure (PKI).

Messages communicated via OCSP are encoded in ASN.1 (Abstract Syntax Notation One) and are usually communicated over HTTP.

**Problems with conventional PKI.**

1. The cost factor:
   Cost of issuance, Cost of Smartcard / USB Token, cost of Card personalization, Cost of deployment

2. The high overheads
   Massive Logistics, Helpdesk support, Cost of Certificates, High upfront and recurrent certificates
3. Lack of mobility
   Conventional PKI is designed for a computer, not for a mobile phone

Thus something better should be discovered / invented.

**Solution: OTPK**

OTPK is One Time Private Key

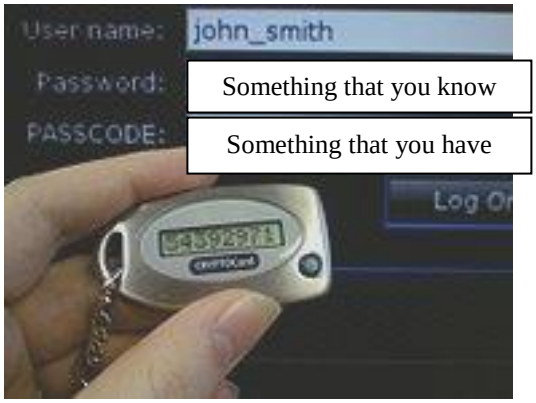
## 4. Salient Features Of OTPK

1. OTPK is only for One-time use. The certificate is short-lived.
2. Each time a signature is needed; the key is generated, certified, used to sign the transaction, and then deleted.
3. Key always remains in client possession throughout the short lifetime, and never stored on a permanent basis.
4. Main security lies in the online certification process where the user would use strong (2-factor) authentication to the CA/RA.

### What is strong (2-factor) Authentication?

Two-factor authentication is the presentation & use of two different kinds of evidences. For example

1. What you have. Such as a token, pen drive, and
2. What you know. Such as a private key, a pin, a password or a passphrase




There are two important phase of OTPK
1. Registration: Verification
2. Actual Signing

Let us consider the first one:

**First phase: Registration**
1. User is issued a 2FA OTP token, OTP sent through SMS, email, etc can be considered but will impact security.
2. Face to face verification, if required, will take place at this stage.
3. The 2FA OTP token will allow the user to authenticate to the CA/RA during the online certification process.
4. Biometric authentication can be utilized under circumstances where remote biometric authentication is secure. i.e. OTPK is not restricted to 2FA OTP, although authentication credentials should be time-bound to ensure freshness of certificate request.

**Second Phase: Signing**

When a digital signature (an asymmetric decrypt operation) on a transaction is required, the user has to download an OTPK module.

OTPK module will

1. Generate public-private key pair.
2. Prompt the user to provide the 2FA OTP credentials
3. Embed the 2FA OTP credential and transaction hash (for time-stamping) within certificate request.
4. Certificate request is end-to-end encrypted for the CA/RA
5. Certificate request is sent to CA/RA
6. CA/RA verifies 2FA OTP credentials, and issues short term (e.g. 5 min) certificate. Certificate contains transaction hash for time-stamping purpose

OTPK module will return the digital signature of transaction and delete the private key.
User now has the certificate and signature, without private key!

**The working of OTPK (One Time Private Key) PKI .**

1. Application server sends the document to be signed to the client server (user) for Digital Signature
2. The user downloads OTPK module and enter 2FA details. (Inserts the card/ token/ pen drive / perform the biometrics as given & instructed by Certificate Authority C.A. / or Registration Authority)
3. The user follows the instructions given by on line C.A./R.A and Generate Certificate request the Digital Signature is created.
4. Application server, from time to time, uses OCSP protocol for look-up and follows up.

The advantages of OTPK over Traditional PKI are:

Easy Interface into 2FA / Biometric authentication

Traditional PKI has 2 different points of authentication – point of issuance & point of signing. Only single point of authentication exists for OTPK

Private Key always in possession of user

Protocol is interchangeable for all asymmetric algorithms

OTPK can be used for RSA, DSA, ECDSA (The Elliptic Curve Digital Signature Algorithm). If algorithm is not suitable e.g. broken, insufficient key length, licensing, platform incompatibility, it can be changed quickly by replacing the

OTPK module. This contrasts with total recall smartcards/tokens which is highly infeasible.

Solution is very scalable

OTPK Backend handles only 1 asymmetric operation (key certification). This can be spread over several sub - CAs in a horizontal scaling infrastructure.

The advantages of OTPK over Traditional PKI are: (cont')

Efficient Pricing model for CA. Since each certificate is tied to a transaction, CAs can charge on a pay-per-use basis.

Differentiation can be:

Mode – online v/s batch processing, per transaction or per authentication session
Timing – peak hour v/s off-peak hours
Loyalty – more usage => cheaper certificates
Branding – Different classes of certificates
Algorithm – Different pricing for different certificates
Level of Insurance / liability

OTPK certificates can be supported on applications that are expecting traditional PKI certificates since OTPK also uses X.509 certificates, barring a possible X.509 extension indicating that status information is not published.

CAs can support both traditional and OTPK PKI and allow both systems to interoperate.

## 5. Issues surrounding OTPK

*Online CA Key*

As compared to traditional PKI, the OTPK CA key is online and certificates are issued in real-time.

Mitigating controls:

Fake certificate requests – Use of strong 2FA with end-to-end encryption for certificate requests.

*User Registration*

In traditional PKI, key is generated once during the registration process. The registration process may require a face-to-face verification.

In OTPK PKI, the authentication token is issued during the registration process. The face-to-face verification step is complied with.

*Secure Time-stamping*

Time stamping is a deliberate process in traditional PKI where the user or server will send the hash for time-stamping.

For OTPK, the transaction hash should be included in the certificate request so that the CA can also provide time-stamping services at no extra processing costs.

*Secure Private key deletion*

The deletion of the key, when the certificate has expired is important. For traditional PKI, proof of private key destruction can be the destruction of the smartcard / token.

For OTPK, besides using properly designed software with FIPS (Federal Information Processing Standards) certification, the indirect way is to ensure that the key cannot be used for any other operation. This is similar to the Secure Time-stamping approach where the transaction hash is included in the certificate, ensuring that improper use will result in a signature verification failure.

## 6. Advantages of OTPK

The advantages of OTPK over existing PKI systems are:

i. No need for smart cards for entities;
ii. Much smaller window of compromise;
iii. A simple and straight forward enhancement of the 2FA with digital signature;
iv. No need for large LDAP systems; (LDAP, Lightweight Directory Access Protocol, is an Internet protocol that email and other programs use to look up information from a server.)
v. No need to maintain CRL; (Certificate revocation list)
vi. Low learning curve;
vii. Easy interface into two-factor / biometric or other authentication solutions;
viii. Private Key always in the possession of the user (comply to many digital signature laws) and protocol is interchangeable for all asymmetric algorithms (RSA, Elliptic curve others) and can be used even on mobile devices;
ix. Very scalable solution (can be deployed to many services that as for today could not fully deployed and use digital signature like, Consumer Banking, e-Bay, PayPal, Google, document management and can easily support millions of users);
x. Efficient and effective business and pricing model for CA (companies like credit cards, online trading, document management, and all the way to many government services can use a central CA to support all their services)
xi. Very easy to change the signing algorithm it take to change the applet only to move from RSA 1024 to 2048, or use same application to use ECC and RSA for full mobility

**Literature Survey:**

The Author has done a literature survey of about 40 good authored papers and more than 12 Books on the subject.

**Research Methodology:**

Primary data by Questionnaire with 5 point grading system and CSF (critical success factor) & KPI (Key performance indicator) Method in a series of seminars and workshops in colleges & corporates selected by purposive sampling method. Statistical method: ($KPI_{before}$ & $KPI_{after}$) With "paired "t" test and level of significance to be 5%; Sample size 500 participants; Secondary data by Library research, Internet search and Mumbai Police records.

## 7. Conclusion

The use of PKI for authentication failed when we tried to deploy it to the consumer users that need a low cost while full mobility solution.
It is much easier to provide a strong user authentication with the two-factor authentication technology.
This will not only enhance the transaction integrity but also make it much more difficult for internal intruders to manipulate the transactions.

The OTPK system is a model shift in PKI technology. It describes a simple and secure mechanism to deploy a large number of certificates across a large user base all over the globe with relatively little cost and logistics.

OTPK technology brings a new concept in which a user will generate a signing key with low cycle time (= key generation + certificate request+ digital signing) takes less than 7 sec.

The OTPK concept is simple to understand. Whenever a digital signature is required, the private key is generated, certified, used to compute the digital signature and immediately deleted. All that remains is the digital signature and the public key certificate from the Certification Authority (CA) that is used to verify the digital signature. There is no possible compromise on the private key.
It is compliant to international digital signature laws. Cyber attack will not come announced. It can attack anybody.
Yes including you and me.
One should be the common man in the society ALERT & AWARE of issues of Cyber attacks and solutions thereof."

## 8. Future Scope

No technology is perfect and no algorithm is crack-proof. Cracker is continuously finding new tools and software to attack. The world is dynamic and threats that we cannot even imagine today may crop up. One day even the strongest security locks are broken. Thus the need of the hour is to be always vigilant, alert & aware about the cyber attack. First acquire the knowledge and disseminate.

The Author can be contacted on vinod_vaze@hotmail.com

## References

[1.] Cyber Crime & Digital Evidence Rohas Nagpal Asian School of Cyber Laws
[2.] Cyber Crime Investigation, Rohas Nagpal, Asian School of Cyber Laws
[3.] Data Communication & Networking B. A Forouzan Tata McGraw-Hill
[4.] e-mail security, Rohas Nagpal, Asian School of Cyber Laws
[5.] Ethical Hacking Ankit Fadia, MacMillan India Ltd.
[6.] Firewalls and Internet Security Cheswick, Bellovin & Rubin Pearson Education
[7.] Intellectual Property issues and Cyberspace Rohas Nagpal, Asian School of Cyber Laws
[8.] Internet – An Introduction, Rohas Nagpal, Asian School of Cyber Laws
[9.] Malware, Incident Prevention & Handling Mell, Kent & Nusbaum, National Institute of Standards & Technology (NIST)
[10.] http://www.demo.com/demonstrators/demo2006fall/79808.php
[11.] ds3global.com/index.php/en/ds3...server/ds3-one-time-private-key
[12.] http://middleware.internet2.edu/pki07/proceedings/03-guan-otpk.pdf
[13.] http://ds3global.com/index.php/en/ds3-authentication-server/ds3-one-time-private-key
[14.] http://www.schneier.com/paper-pki-ft.txt Ten risks of PKI