ARRAY Logo

# Bridging Strong Authentication with PKI

**By TAN Teik Guan, CTO, Data Security Systems Solutions PL**

Web: www.dsssasia.com
Email: teikguan@dsssasia.com

*Teik Guan has many years of hands-on experience in designing and implementing data security solutions for many highly-sensitive projects including the Interbank RTGS Systems, Cheque Clearing Systems and several Internet banking and trading systems. Teik Guan is well-versed in the niche area of cryptographic security programming and integration, having developed numerous successful products such as CAs, smartcards (Javacard), HSMs, Authentication Servers, etc. Teik Guan holds a MSc from the National University of Singapore.*

## Abstract

**With the banks investing heavily in strong 2-factor authentication infrastructures for their Internet Banking systems, there must be a greater business justification for implementing and maintaining this investment. This can be materialized through the banks exploiting the 'secured' Internet channel to carry out larger volume and higher-value transactions with their clients. The use of PKI (Public Key Infrastructure) for digital signatures on these transactions will give the banks the legal recourse and protection (through the digital signature laws) to launch more products over the Internet or push for more B-to-B straight-through processing for greater business efficiencies.**

**The challenge therefore is how to bridge authentication with PKI, without the need to deploy the expensive and cumbersome-to-manage smartcards, and yet be compliant to the Digital Signature Laws. In this paper, we will describe how a strong authentication infrastructure can be leveraged upon to deploy a very dynamic PKI system for digital signatures, without the need for smartcards. The technology is called, One Time Private Key (OTPK).**

### Introduction

There are 2 main schools of thought when it comes to 2-factor authentication. One school advocates the use of one-time password tokens that display unpredictable one-time passwords, typically between 6 to 8 digits, which can be presented for verification as proof of current possession of the token. Products that fall into this category include hardware tokens (e.g. RSA SecurID, VASCO Digipass, ActivCard tokens), Pin Mailers, one-time passwords via SMS, S/Key, etc. The other school prefers the use of smartcards or USB tokens to implement a PKI system that can be used for authentication, encryption and digital signatures.

The significant advantages in using one-time password technologies over PKI technologies are that they are extremely mobile for the user, and cheaper to deploy and maintain. PKI technologies suffer from the

need to install some form of recognizable smartcard reader or driver in the target machine before they can be used. The cost of deploying and maintaining a smartcard-based PKI solution is much higher due to the underlying logistics difficulties and steep user learning curve. On the other hand, PKI technologies are able to provide transaction non-repudiation through the use of digital signatures, a key component in allow high value and larger volume transactions to happen on the electronic medium.

In this paper, we introduce the One time Private Key concept, a revolutionary method to implement and deploy PKI using only the one-time password token infrastructure, ensuring the same, if not higher, level of integrity and non-repudiation of the transactions, and yet not needing to incur the costs and logistics involved in deploying smart card solutions.

## The OTPK Concept

The main concept behind OTPK is that the Private key is a 'One-Time Private Key' (OTPK).

In a typical PKI (or asymmetric key) system, each user has to initially register securely (e.g. using one-time authorization code in the case of Entrust) to the Certification Authority in order to be issued the digital certificate. Subsequently, with the possession of the certificate, the user can use the Private Key, for the duration of the certificate validity, to compute a valid and recognized digital signature for a transaction.

In contrast, the Private Key in the OTPK system is for one-time or per-session use only. In the OTPK system, each user will always generate a new Private Key and register and authenticate securely with the Certification Authority in order to be issued with a digital certificate, for every transaction or for every session. This is where the "bridging" happens. Instead of being issued one smartcard to contain a one-year certificate, each user is issued some means of strong authentication (e.g. one-time password tokens or biometrics) to request for certificates each time a digital signature is required. Once the Private Key is used or when it is expired with the session, the Private Key is erased and discarded. There is no need to permanently store the Private Key in any media. While such a process sounds onerous, the overheads are actually not much more than any mobile credential solution, but the benefits are tremendous.

Note that there is no compromise in terms of security since the issuance of the certificate is done in the same manner for both the typical PKI and OTPK, except that the number of certificate requests is much higher in the OTPK case. Face-to-face verification, which is usually done during the issuance of the smartcard can also be done for OTPK during the issuance of the authentication token.

## Advantages of OTPK

The advantages of OTPK over the existing PKI systems are:

- **No need for smart cards for clients**

  In the OTPK system, since the users' Private Keys are generated only when needed, and discarded after use, there is no need for traditional smart cards (or USB tokens) to store and protect the Private Keys. This represents very significant savings in terms of costs, resources and time overheads in implementing and maintaining a PKI system.

- **Much smaller window of compromise**

  In the OTPK system, the duration of validity of the Private Key and certificate is extremely short. Also, the number of digital signatures generated from the Private Key is very low; typically the Private Key is used to generate only one or a few digital signatures for its lifetime. Moreover, the Private Key is erased after use. The combination of short duration, lack of substantial signature data and absence of any key storage makes the OTPK system more difficult to compromise.

- **No need for large LDAP systems**

In a typical PKI system, the CA, after issuing the user's certificate, would lodge the certificate with a LDAP system. This is to allow other party to retrieve the certificate for verification purposes. Such LDAP systems have to be able to handle large amounts of load in order to support the verification process.

In the OTPK system, since each certificate has a small and limited time validity, the use of the LDAP for storing and publishing the users' certificates is not as relevant. Instead, the certificate could be attached with the digital signature in the transaction.

- **No need to maintain CRL**

  In a typical PKI system, a CRL (Certificate Revocation List) and/or OCSP (Online Certificate Status Protocol) mechanism has to be in place to maintain the up-to-date status of the certificates. For example, if a user has lost the Private Key, the corresponding certificate should be revoked, and listed in the CRL so that corresponding parties do not rely on the certificate from that point onwards. However, the CRL and OCSP mechanisms add significant overheads to the entire PKI process.

  In the OTPK system, the CRL and OCSP for the user certificates are no longer relevant since the Private Keys and certificates have limited time exposure and would not be compromised. This is similar to a number of short-lived certificate implementations.

- **Low learning curve**

  One of the big problems with existing PKI implementations is the need to educate and re-educate the users in using the PKI technology. Most individual users find PKI rather confusing with the need to understand how to use smart cards (e.g. installing smart card readers, entering a pin, changing the pin on a regular basis, etc), and how to use certificates, and what to do when the certificate expires, etc. This takes up significant time, costs and resources to help the users.

  For the OTPK system, all the confusing cryptographic technology and PKI protocols are abstracted from the user and the user only needs to decide that a transaction needs to be digitally signed, and to authenticate with the CA. All the complexity is either made redundant by the OTPK design or handled easily by the user-side application's interaction with the CA.

- **Easy interface into 2-factor / biometric or other authentication solutions**

  Strong authentication should be implemented to ensure that only the correct user could carry out a digital signature.

  In a typical PKI system, there exists two points of authentication, one with the CA for the initial certificate issuance (which is carried out once in a long time), and one with the media (e.g. smartcard) containing the Private Key for using the Private Key (which is carried out as and when the Private Key needs to be used. Authentication to the media is usually static PIN-based, as it is the media that enforces the authentication. If the protection of the media requires more complicated or stronger authentication, then a lot more complexity have to be built into the media, resulting in higher costs. Moreover, not all media can support all forms of strong authentication.

  In the OTPK system, only one point of authentication, which is to authenticate with the CA, is needed. It is carried out as and when a Private Key is needed to be used. Since the authentication can be centralized to the CA or a collection of CAs, there is economy of scale in implementing a strong authentication (such as 2-factor, biometric, etc) to the CA, and the cost can be shared across a large pool of users. There is also no constraint on the media, which makes it easier to integrate a strong authentication mechanism into the OTPK system.

- **Private Key always in the possession of the user**

  Many of the legislation regarding Digital Signatures and PKI explicitly require that the user's Private Keys by always in the possession and control of the user. Such requirements imply that some of the mobile credential solutions, which allow for the Private Keys to be centrally escrowed or stored on behalf of the user, to be not recognized as compliant to the Act.

  The OTPK system relies on a user-side program to generate and temporarily store the Private

Key for the short duration that the Private Key is used. In the entire process, the Private Key remains in the possession and control of the user.

- **Protocol is interchangeable for all asymmetric algorithms**

  The OTPK system does not differentiate between different asymmetric algorithms and allows for users using different asymmetric algorithms (e.g. RSA, DSA, ECDSA, etc) to participate within the same PKI. This means, for example, that one user can be using RSA to perform digital signatures while another user can be using ECDSA. Since the CA handles the certification collectively at the point of performing the digital signature, the OTPK solution is flexible enough to allow different users using different algorithms to participate together.

  Also, in the event that an algorithm is deemed undesirable, due to whatsoever reason such as cryptographically broken, insufficient key length, licensing, poor performance, platform constraints, etc, the user can easily use a different algorithm or key length without affecting all the other participating users. The CA may also quickly and seamlessly migrate users from using one algorithm to another without affecting the PKI or the PKI operations.

  This flexibility allows different users using different applications and platforms, e.g. from large servers to personal computers to mobile devices, etc, to participate in the PKI. This also allows a single PKI deployment to support different algorithms depending on the locality, jurisdiction, or local laws (e.g. some countries regulate the use of certain cryptographic algorithms).

  Such flexibility is currently not practical within the existing PKI system which rely on smart cards or some media due to logistics, costs, resources, etc.

- **Efficient and effective business and pricing model for CA**

  In the typical PKI, the CA charges on fixed-duration (e.g 1 year) basis. However, since the Private Key to the certificate can be used to sign many transactions, the CA charges a significant amount of money per certificate. Such a pricing model does not efficiently charge according to the actual usage since a user that uses the Private Key regularly versus another user that uses the Private Key rarely are charged the same amount.

  In the OTPK system, since the certificates are issued each time a Private Key is used, the CA can charge a much smaller amount for each certificate. Such a pricing model will mean that users who carry out digital signing more often will incur more charges, and vice versa. This results in a fairer and more acceptable pricing model. It also allows CAs to price the certificates and services differently for different applications such as the following:

  - **Mode.** Online certification versus batch certification are priced differently
  - **Timing.** Certification requests during peak hours will incur higher charges
  - **Loyalty.** The more certificates are requested, the cheaper the cost of each certificate
  - **Branding.** Different classes of certificate with different certification policy are priced differently.
  - **Algorithm.** Certificates for different algorithms are priced differently.
  - **Insurance.** Price of certificate includes insurance on the transaction that is tied to the certificate.
  - **Duration.** One-time use versus per-session use certificates cost differently

  The CA may also choose to issue both traditional PKI as well as OTPK certificates and allow both these systems to interoperate, ensuring the maximum flexibility for the CA to adjust the business model.

## Ending Remarks

The OTPK system is a paradigm shift in PKI technology for Internet transactions. It describes a simple and secure mechanism to deploy large number of certificates across a large user base, with relatively little cost and logistics.

The downside of the OTPK System is the need to be online while carrying out the transaction. While

this eliminates the use of OTPK for off-line signing applications, this shortcoming would not impact the application of OTPK for its intended use in Internet Banking transactions.

There are already a number of variations of such dynamic PKI being implemented in the market. My company, DSSS, has developed and patented some of these implementations.