AT.Sign

Application Engine for Digital Signing using PKI Technologies

White Paper

iASPEC Software Limited
Unit 511, Lakeside 1
8, Science Park West Avenue
Hong Kong Science Park
Shatin, N.T. Hong Kong

TABLE OF CONTENTS

1. INTRODUCTION 2

PURPOSE OF THE WHITE PAPER 2

WHAT IS DIGITAL SIGNING 2

MAKING "DIGITAL SIGNING" EASY 5

2. A QUICK OVERVIEW OF AT.SIGN 7

WHAT IS AT.SIGN 7

BENEFITS TO THE USERS 8

AT.SIGN COMPONENTS 9

3. FREQUENTLY ASKED QUESTIONS 13

WHAT ARE THE DOCUMENT TYPES SUPPORTED BY AT.SIGN 13

WHAT IS THE CERTSTORE 13

HOW TO INTEGRATE AN APPLICATION WITH AT.SIGN 14

WHAT IS THE OTP TECHNOLOGY EMBEDDED IN AT.SIGN 15

1. INTRODUCTION

PURPOSE OF THE WHITE PAPER

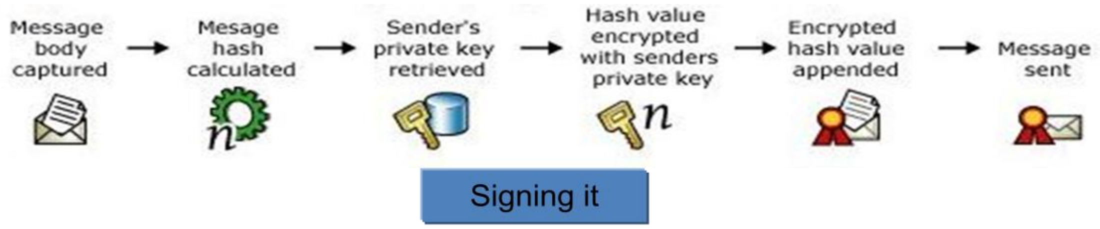
This White Paper is written to assist its readers in examining the Public Key Infrastructure (PKI) system and to gain an understanding on its application in digital signature.

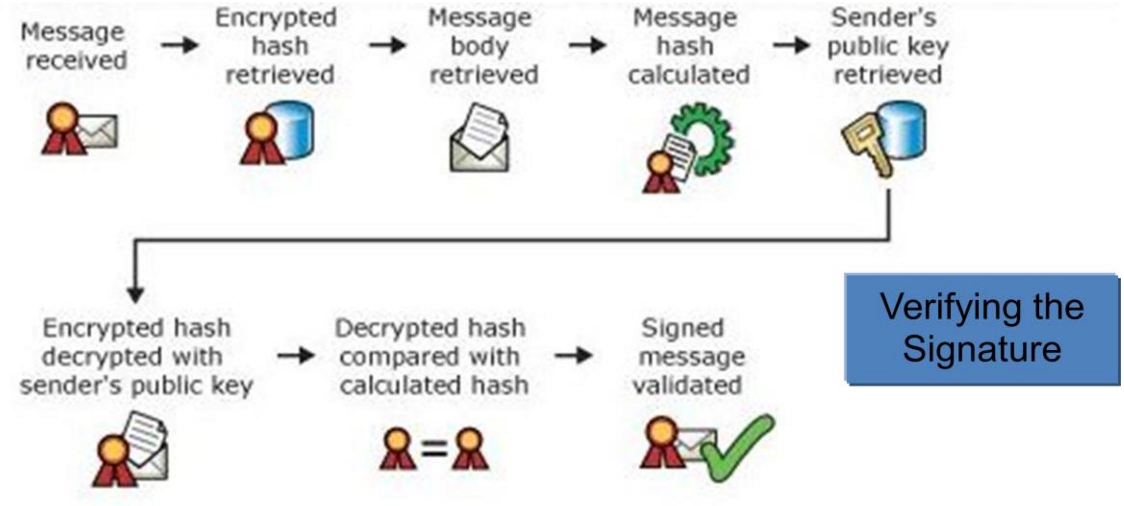
The target audience of this Whitepaper includes but not limited to corporate management and IT executives who are involved in technology evaluation, integration and purchase decisions. Some basic level of understanding in information security is required for the audience to grasp the essence of this Whitepaper.

WHAT IS DIGITAL SIGNING

Digital Signing is the commonly accepted technology for protecting integrity and proving authenticity of electronic documents. It is analogous to the traditional manual signatures that people have on hard copy documents throughout the histories of many cultures.

The basic principle behind Digital signing is the application of an asymmetric cryptographic calculation on the document content, using a pair of "keys" (known as the private key and public key pair) that are uniquely assigned to the "signer" of the document. The following diagrams briefly explain how digital signing works:


Message body captured
Mesage hash calculated
Sender's private key retrieved
Hash value encrypted with senders private key
Encrypted hash value appended
Message sent
Signing it



This asymmetric sharing of a secret or secrets, in the form of the private key and public key; as well as the use of these keys to perform digital signing is generally considered as one of the best ways to establish "non-repudiation" on the electronic information exchanged between the involved parties. These key pairs are commonly referred to as the Digital Certificates

What is a Digital Certificate :

- A digital certificate is a digital form of identification, much like a passport or ID card. A digital certificate is a digital credential that provides information about the identity of an individual or an entity (e.g. a Server) with other support information.
- There is an ITU standard, known as X.509 covering the various technical aspect of a digital certificate.
- A publicly recognized digital certificate is generally issued by an authority, referred to as a certification authority (CA).

The Public Key Infrastructure (PKI) refers to a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke these digital certificates.

PKI provides the means for digital certificates to be used by issuing certificates and making them accessible through a directory. PKI also validates digital certificates by verifying the authenticity of the certificate, the validity of the certificate, and that the certificate is trustworthy by virtue of the issuing certificate authority (CA).

Many nations and economies, including the Hong Kong SAR, have enacted legislations accepting “Digital Signature” as having the same legal standing as physical signatures in hard-copy forms.

Quick Facts:

- The Hong Kong Electronic Transaction Ordinance (ETO) was enacted on 5 January 2000.
- The ETO 2004 (Amendment) Ordinance was enacted on 30 June 2004.
- The Hongkong Post Certification Authority is a recognized certification authority by virtue of the ETO.

MAKING "DIGITAL SIGNING" EASY

One of the common perception hampering the wider adoption of Digital Signing and the PKI infrastructure is that the technology is difficult to implement and its applications are quite inconvenient for layman to use. A frequently voiced complaint is the inconvenience that people have experienced in the safe-keeping of the "keys" that were assigned to them. The following scenarios are very real concerns that users have experienced:

1. If the digital certificates were distributed in the form of smart cards (e.g. the Hong Kong ID Card), then purpose-built card readers are required to read these keys from the smart cards. This requirement places severe restriction on the use of the digital certificate in an open environment.

2. If they were loaded into the client devices (e.g. the PC) that the users own, then the use of the digital certificates is tied to these client devices. Moreover, when the security of these client devices is compromised, the digital certificates can be stolen without the user's knowing.

3. If they were preloaded into portable storage devices (e.g. USB flash drives) to give the users some degree of mobility in the use of the digital certificates, it runs the risk that the loss of these portable devices will result in the loss of the secrets stored on them. Moreover, the insertion of these devices into a PC that is not necessarily secure can also present as an unacceptable security risk.

4. In some situations, the digital certificate is hidden beneath a smart USB device. These devices come with embedded computing capabilities within them for performing various

encryption, decryption, signing and verification functions without exposing the digital certificate outside of it. Outside applications interact with these devices through different forms of programming interfaces. The disadvantage of this approach is their high degree of dependence on the operating system environment for such programming interface to work. Changes in operating system may cause such rigidly implemented interface to fail.

5. Many of today’s mobile devices do not support USB ports through which the user can insert a device where the digital certificates may have been stored. This trend in mobile device design has limited the scope of applicability of digital certificates that are stored in any form of USB devices.

All these perceptions and concerns are very real and they have hampered the broader adoption of Digital Signing and PKI for many years.

To fundamentally solve these problems, we must find a sufficiently secure way to store these digital certificates and to give the users the needed mobility when accessing them for digital signing and other purposes. In practice, it must not tie the user to a particular client device where the certificate is stored. Ideally, it must not rely on the use of some special hardware that is attached to the client device for the reading and decoding of these digital certificates.

The AT.SIGN is a software solution that is designed to address these concerns and to solve the associated problems.

2. A QUICK OVERVIEW OF AT.SIGN

WHAT IS AT.SIGN

AT.SIGN is a new approach for integrating digital signing features into various software applications. It is provided in the form of a software library with easy-to-use interfaces through which the target software applications can implement digital signing requirements. It is supported by a highly sophisticated and secure scheme for the management of the digital certificates that are used in the signing actions. Full audit trail of the signing actions are kept as an added degree of security in proving authenticity of the signed documents.

Some of the key features of AT.SIGN:

- AT.SIGN uses a secure CertStore for the storing of users' Digital Certificates. This secure CertStore can be physically separated from the AT.SIGN server and is protected by strong encryption.

- The access to the Secure CertStore is protected by encryption keys that are further protected by a One-time Password (OTP) accessing scheme. This is a much stronger scheme compared to the standard protection of static password that is commonly used for digital certificate access.

- With the digital certificate centrally and securely stored, software applications can gain access to the certificate indirectly through networks for the performance of various document signing and verification transactions. These software applications are typically protected by OTP-based authentication schemes for stronger security on the access control.

- This approach opens up the possibility for the user to indirectly access the digital certificate through authorized applications connected from many forms of online devices. This includes the smart phones and tablet PCs on which the storage of digital certification is either technically impossible or is considered as unsafe to do so even if it could be done.

- Moreover, the access to the digital certificate, its use in any of the digital signing and verification actions, as well as certificate installation and invocation events are securely kept in the audit trail maintained by AT.SIGN. This feature provides additional level of security in the proof of authenticity of documents signed by the AT.SIGN software.

BENEFITS TO THE USERS

Companies implementing or switching their digital signing over to AT.SIGN are very satisfied with the product and they have reported the following benefits:

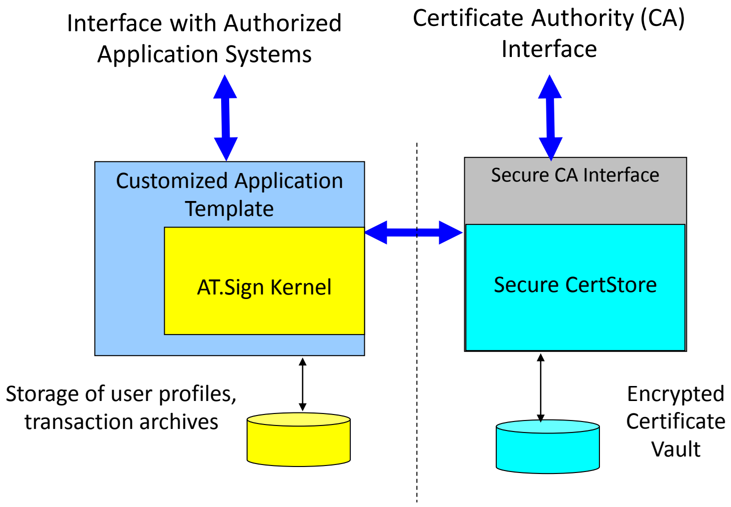
Increased Security — The in-built one-time password (OTP) feature provided by AT.SIGN has significantly improved the security in the management of the digital certificates. Moreover, the audit trail function gives an added degree of security to the target application system. These audit trail records can be reviewed by the authorized users and administrators for preventive and forensic analysis of security breaches.

Easy and Flexible Deployment — AT.SIGN supports Java-based application program interface (API) and Web Services invocation schemes. Target applications can easily integrate with AT.SIGN and to take full advantage of the functions and features provided by the software.

Improved Business Processes	As the digital certificates are centrally stored, it has significantly reduced the administrative burden and costs associated with certificate issuance, replacement and revocation processing.

AT.SIGN COMPONENTS

Architecturally, AT.SIGN comprises the following components or


Interface with Authorized Application Systems
Certificate Authority (CA) Interface
Customized Application Template
AT.Sign Kernel
Secure CA Interface
Secure CertStore
Storage of user profiles, transaction archives
Encrypted Certificate Vault

subsystems as shown in the diagram below:

Some details of these components are highlighted below:

AT.SIGN Kernel

- Maintaining the profiles of registered users of AT.SIGN;
- Performing the digital signing services in accordance to the electronic signature standards supported (e.g. XML signing, PDF signing….);
- Performing signature verification services;
- Journaling and archiving of the signing and verification actions as requested and other key events of the system;
- Providing a secure interface for the viewing of the audit trail and archive.

Secure CertStore

- Managing the secure storage of the digital certificates for all registered users;
- Interfacing with the CA through the customized CA interface module;
- Managing the encryption and storage the digital certificates in the Digital Certificate Vault;
- Retrieval of the digital certificates for signing and verification services.

Customized Application Templates and Interfaces	• User authentication based on the adopted security scheme of the application systems when connecting to the AT.SIGN for its services; • An application-oriented Web Services interface and Client Library to facilitate the integration of AT.SIGN services with the application systems; • A template (in the form of a sample program) that can assist designers and implementation engineers in the customization of the document standards and workflow requirement to suit the needs of the target applications.
Web Service API and Client Library	• Web Services API and Client Library that can be used in the integration with the target applications systems; • Customized features can be added to the library based on the customization needs of the applications.
Certificate Authority (CA) Interface	• A secure channel for interfacing with the CA can be implemented (for example, the process of digital certificate distribution can be automated through this interface between the CA and the AT.SIGN system); • Performing Certificate management instructions from the CA (e.g. revocation, downloading of blacklist…..)

Encrypted Certificate Vault	• Encrypted storage of the digital certificates on hard-disk and/or the database files to prevent the thief or loss of these devices and data.

3. FREQUENTLY ASKED QUESTIONS

WHAT ARE THE DOCUMENT TYPES SUPPORTED BY AT.SIGN

The latest version of AT.SIGN supports the following document signing functions:

1. The signing of free-form files including the document digests of other documents. This is done by encrypting these files using the private key of the digital certificate;
2. The signing of an XML document as defined under the W3C standards[1];
3. The signing of PDF document as defined under the ISO 32000-1 standards[2].

WHAT IS THE CERTSTORE

One can draw analogy of the CertStore with the vaults of a bank where safe deposit boxes of various customers are securely located and protected in a similar way, CertStore maintains these electronic "safe deposit boxes" that are uniquely assigned to each registered user of AT.SIGN. Digital certificates of these users are locked inside these individually owned "safe deposit boxes".

AT.SIGN allows user to store multiple certificates in these "safe deposit boxes" for the different role-based identity that he/she may has.

[1] for details: http://www.w3.org/TR/xmldsig-core/

[2] For details: http://www.iso.org/iso/catalogue_detail.htm?csnumber=51502

When a user needs to access these certificates, he/she will go through a "gatekeeper" of the AT.SIGN software for authentication of his/her identity. This authentication is done using OTP. This scheme is much stronger than the use of static PIN that is commonly found in most PKI implementations.

While CertStore can be installed together with the other components of AT.SIGN in a single server, it can also be separately installed in isolated hardware to further strengthen the security of the entire system.

HOW TO INTEGRATE AN APPLICATION WITH AT.SIGN

The AT.SIGN solution is designed in the form of an “App Engine”.

"App Engine" used in the current context can be understood as a set of software services that can be invoked, in a loosely couple form, by a collection of applications. It aims at making the target applications easier to design, develop and to maintain by factoring out some of the core features and more complex processes needed in these applications. The following are some of the basic characteristics of this AT.SIGN App Engine:

It provides a level of abstraction for the core processes and basic services of digital signing that are needed in these target applications.

These functions (can be referred to as "services") are implemented in a way such that the lower-level details are hidden from the upper level applications. This "separation of concerns" provides clear and well-defined boundaries isolating the internals of the App Engine from the exposed outside view that the applications can use in invoking these functions.

The functions are sufficient fine-grained to promote reusability; they are also modular in nature to support service autonomy; highly composable to form more complex composite functions; and interoperable with different technologies that the users may choose to implement the target applications.

This AT.SIGN App Engine is providing a set of web services that are designed specifically to support digital signing of electronic documents in any applications. This Web Services based interface can be used for integration with applications developed using various types of technologies and languages.

For integration with applications built using Java, AT.SIGN also provides a set of Java-based API. Native Java applications can integrated with AT. Sign through this set of API client library.

WHAT IS THE OTP TECHNOLOGY EMBEDDED IN AT.SIGN

Embedded within AT.SIGN is another iASPEC award winning software product, the AT.PASS.

AT.PASS is based on the use of software token for the generation of one-time-password (OTP). It supports tokens that are distributed and installed into PCs, smart phones, tablets, and various types of mobile devices (including iOS, Android and Windows Mobile devices). It also supports CueCard that are delivered to the user's registered email box upon specific request. CueCards containing a list of pre-generated OTP. These pre-generated OTP can be used in sequence by their designated users within the validity period of the CueCard.

Compared to other hardware token based solutions, our choice of software token has greatly reduced the overall cost in deploying advanced OTP technology serving user authentication purposes of many different application types and scenarios.

The version of AT.PASS embedded within AT.SIGN is licensed for the AT.SIGN usage only. Should the customer desires, AT.PASS can also be separately licensed as a product. Many customers are using it as an OTP-based user authentication solution and it is deployed in a great variety of enterprise online application systems.