# AT.SIGN

## Digital Signature Solution
## Based on PKI Technologies

### Contact Info

Aalfa Tech Limited
P.O. Box 93915, Dubai, U.A.E
Phone: +971 4 342 9240
http://www.aalfa.tech
info@aalfa.tech

aalfatech

iASPEC

# AT.SIGN

## Digital Signing

Digital signing is a commonly accepted technology for protecting integrity and proving authenticity of electronic documents. 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. 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.

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. Many nations and economies, including the Hong Kong SAR, have legislations enacted for accepting “Digital Signature” based on digital certificates issued by recognized Certificate Authority (CA) as having the same legal standing as physical signatures in hardcopy forms. However, the perceived and real difficulties in adopting and using PKI have hampered its wider adoption of digital signing.

## The AT.SIGN Solution

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.

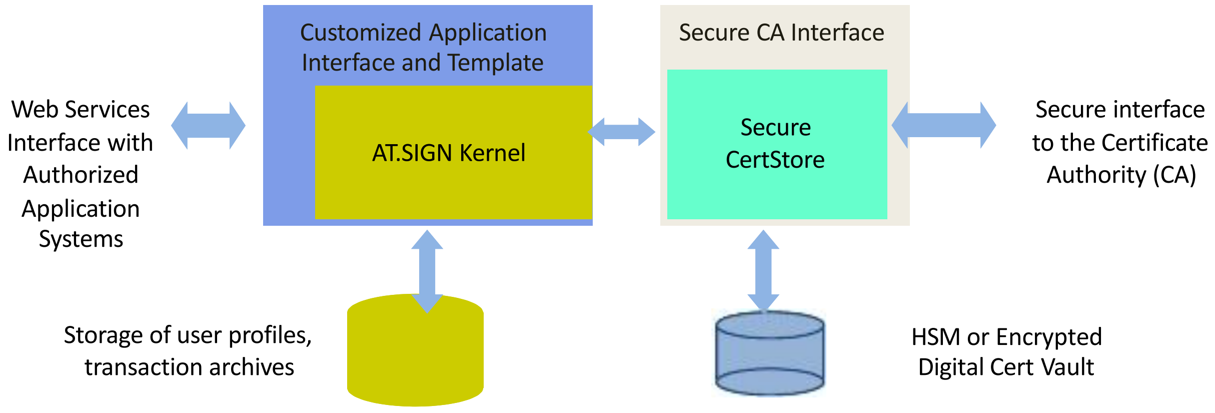
Customized Application Interface and Template
AT.SIGN Kernel
Secure CA Interface
Secure CertStore
Web Services Interface with Authorized Application Systems
Secure interface to the Certificate Authority (CA)
Storage of user profiles, transaction archives
HSM or Encrypted Digital Cert Vault

Figure 1. The subsystems of AT.SIGN

## Feature Highlight

AT.SIGN is designed for small to large scale deployments. Key features of its subsystems are:

### AT.SIGN Kernel

- Maintaining profiles of registered users and making use of the AT.Pass or other OTP services for user authentication;
- Performing the signing services in accordance to the electronic signature standards supported (e.g. XML signing , PDF signing….);
- Performing signature verification services;
- Journaling and archiving the signing and verification actions and other key events;
- Providing a secure interface for retrieving and viewing of audit trail archive.

### HSM Integration and 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 or in a HSM;
- Retrieval of the digital certificates for performing the signing and verification services.

### Web Services 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 upon customization.

### Application Interface and Templates

- An application oriented Web Services interface and Client Library to facilitate the easy integration of AT.SIGN services with the application systems
- Application templates are provided to assist designers and implementation engineers in the development of applications with customized workflow requirements.

### Secure CA Interface

- A secure channel for the direct interface with the CA for the acceptance of Digital Certificates for storage at CertStore as directed and on behalf of the users
- Performing Digital Certificate management instructions from the CA (e.g. revocation, downloading of blacklist…)
- Encrypted storage of the Digital Certificates on hard disk and/or the HSM to guard against any theft or loss of these devices and data

### AT.SIGN Server Requirements

| | |
|---|---|
| Operating System | Any OS supporting Java JRE 1.6 and above |
| Database | • MySQL 5.0 and above;<br>• PostgreSQL 8.4 and above;<br>• MS SQL 2008 and above<br>• Oracle 9i and above<br>• DB2 |

The iASPEC Technologies and Services group is a leader in supplying OTP-based (One-time Password) identity authentication solutions and PKI-based digital signature platform products.

Brief history of the Group in the OTP and PKI technology areas:

- 1988 – Founding of the Company in Hong Kong.
- 2005 – Released AT.Pass , an award winning One-Time-Password authentication solution.
- 2009 – Released the AT.Sign digital signature solution. It is currently deployed by government departments, public service organizations and large enterprises in Hong Kong and Mainland China to support various digital signature applications.
- 2011 - Launched SecurDS, a cloud-based digital signature service based on the AT.Sign technology,
- 2009 - Involved in the early discussions on the e-Cheque initiative through the HKPKI Forum.
- 2013 - Received the Most Valuable Companies Award from Mediazone Group for its achievement in software services.
- 2014 – Extended the standard AT.Sign product to support e-Cheque.
- 2016 – Extended the standard AT.Sign product to support digital ledger in the form of blockchain.

aalfatech

iASPEC