数字签名

“数字签名”是一种被普遍接受的技术，用于保护电子文档的完整性及验证其真实性。数字签名背后的基本原理是使用非对称加密算法计算文档内容，它使用了一对“钥匙”（私钥和公钥），是分配给文档“签署者”的唯一“钥匙”。数字签名，它使用了私钥和公钥，非对称共享了一个或多个秘密；这种使用私钥和公钥的技术，通常被认为是相关方在电子信息交换中建立“不可否认性”的最佳途径之一。这一对“钥匙”通常被认为是数字证书。

公钥基础设施(PKI)是指一系列用于生成、管理、颁发、使用、存储和撤销数字证书的硬件、软件、人员、政策和流程。许多国家和经济体，包括香港特别行政区，均有已生效的法规承认数字签名具有与物理签名相同的法律地位。然而，一些观念上和实际上的困难仍存在于PKI的应用和使用中，正是这些困难，阻碍了PKI在数字签名中的广泛应用。

AT.SIGN 解决方案

要从根本上解决这些问题，我们必须找出一个足够安全的方法存储数字证书，并赋予用户在使用证书时所需的流动性。实际上，我们不应该将用户与存储证书的某个特定设备绑在一起。最理想的是，它不依赖一些与客户端设备相连的特定硬件来读取、解码数字证书。

AT.Sign就是为了解决这些与数字签名相关的问题而设计的软件解决方案。

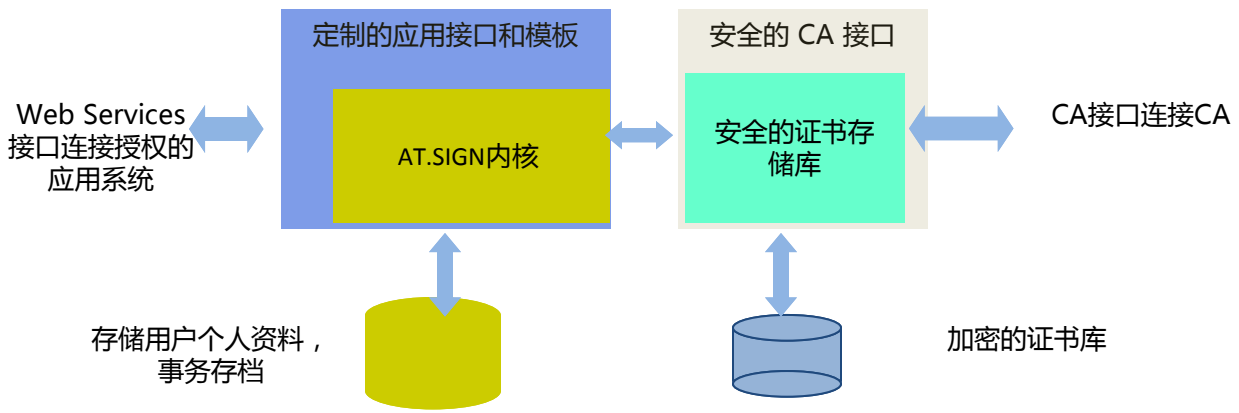

图 1. AT.SIGN子系统

AT.SIGN – 基于PKI技术的数字签名解决方案

产品特性

AT.SIGN为不同大小规模的部署而设计，各子系统的主要特性如下：

AT.SIGN 内核

- 维护注册用户的个人资料以及使用AT.Pass一次性密码服务进行用户认证；
- 根据所支持的电子签名标准（如XML签名，PDF签名…）执行签名服务；
- 执行签名验证服务；
- 对签署和验证操作以及其它关键事件进行记录和存档；
- 提供一个安全接口以检索查看审计跟踪的存档。

安全的证书存储库

- 为所有的注册用户管理证书的安全存储；
- 通过定制的CA接口模块连接CA；
- 管理加密的证书库或HSM中的数字证书的加密和存储；
- 为签署和验证服务检索数字证书。

Web Services API 与 Client Library

- Web Services API 和Client Library可用于与目标应用系统的整合；
- 根据定制需求，可在library中添加要定制的功能。

应用接口和模板

- 面向应用的Web Services接口和Client Library，使AT.Sign与应用系统易于整合；
- 提供应用模板，帮助设计师和实施工程师使用定制的工作流程需求开发应用。

安全的 CA 接口

- 根据用户指示，AT.Sign通过CA接口接受来自CA的数字证书并将证书存储在证书存储库中，直接地建立了AT.Sign与CA之间的安全连接；
- 执行CA的证书管理指令 (例如，撤销，下载黑名单…)；
- 数字证书被加密存储在硬盘和/或HSM中，以防设备和数据被盗或丢失。

AT.SIGN 服务器的系统要求

操作系统	任何支持Java JRE 1.6 或以上的操作系统
数据库	• MySQL 5.0 或以上； • PostgreSQL 8.4 或以上； • MS SQL 2008或以上； • Oracle 9i或以上。

地址：香港新界沙田香港科学园二期科技大道西8号尚湖楼5楼511室
电话：+852 3125-9000
传真：+852 2668-2166

http://www.iaspec.com