AT.SIGN

使用 PKI 技术的
数字签名应用引擎

白皮书

永泰信息技术服务有限公司
香港新界沙田
香港科学园二期
科技大道西 8 号楼
尚湖楼 5 楼 511 室

目录

1. 介绍

本白皮书的目的

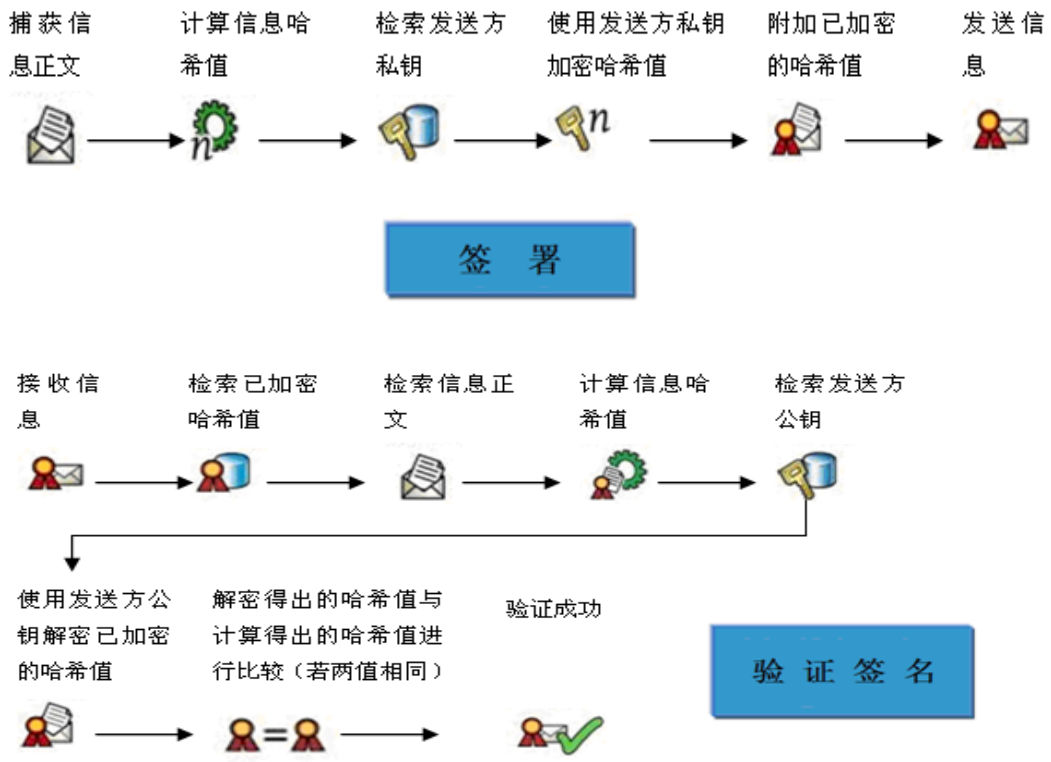
本白皮书旨在帮助读者剖析公钥基础设施(PKI)系统，并理解 PKI 系统在数字签名解决方案中的应用。

本白皮书可供公司管理层和 IT 主管阅读，供他们在技术评估、整合与采购过程中参考；也可供其他感兴趣读者阅读。读者需理解一些信息安全的基本知识，以便掌握本白皮书的精髓。

何为数字签名

数字签名是一种被普遍接受的技术，用于保护电子文档完整性及验证其真实性。数字签名类似写在硬副本文档上的手写签名。

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”。下图简单解释了数字签名的工作原理。



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。

何为数字证书：

- 数字证书是电子形式的身份证明，类似于护照或身份证。它除了提供个人或实体（如，服务器）的身份信息，还提供了其它支持信息。
- X.509 标准，国际电信联盟（ITU）设计的标准；它定义了数字证书的格式，包含了：版本号、序列号、签名算法、颁发者、有效期限、等不同信息。
- 受到公认的数字证书通常是由某权威机构颁发，而此机构则被称为认证机构(CA)。

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。

PKI 提供了使用数字证书的方法，包括：颁发证书和获取证书。不仅如此，PKI 还借助 CA，通过验证证书的真实性、有效性和可靠性，使数字证书生效。

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。

小知识:

- 香港政府于 2000 年 1 月 5 日制订了《香港电子交易条例》。
- 《电子交易(修订)条例 2004》自 2004 年 6 月 30 日起生效。
- 《香港电子交易条例》确立了香港邮政证书颁发机构为一个认可的证书机构。

然而，数字签名和 PKI 设施的应用却受到阻碍，人们认为：此技术难以实施，且对外行人而言，其应用的操作相当不方便。人们还常常抱怨“钥匙”的安全保管很不方便。以下情景真实地反映了用户所遇到的问题：

1. 如果数字证书以智能卡的形式颁发（例如香港身份证），则需要专用读卡器以读取智能卡中的密钥。在开放环境下，读卡器的需求严重制约了数字证书的使用。

2. 如果将数字证书载入用户自己的客户端设备（如个人计算机），则意味着数字证书与该设备绑在一起，从而限制了证书的使用场合。而且，当客户端设备的安全性受到威胁时，数字证书可能会被盗，而用户却无法察觉。

3. 如果将数字证书预载入便携式的存储设备（如 USB 闪盘），显然，用户在使用数字证书时具有了一定的流动性。可存在的风险是，一旦丢失这些设备，存储其中的秘密也将一同丢失。而且，将这些设备任意插入其它计算机的行为并不安全，可能会导致巨大的安全性风险。

4. 某种情况下，数字证书隐藏在智能 USB 设备当中。这些设备可在其内部实现加密、解密、签名和签名验证；换句话说，数字证书的使用始终在 USB 内执行。在这种情况下，外部的应用会通过不同的程序接口与 USB 连接和通信。然而，这种方案却存在的一个劣势：要使这样的程序接口得以工作，对操作系统环境的依赖性必然很高。面对如此严格的接口实施，操作系统的更替可能导致接口失效。

5. 目前许多移动设备都不支持 USB 端口，理想情况下，通过 USB 端口，用户可接入存储了数字证书的设备。移动设备的这种设计趋势，使存储在 USB 设备中的数字证书难以使用，限制了数字证书应用范围。

所有这样体验和考量都是实实在在的，许多年来，正是这些体验和考量，阻碍了数字签名和 PKI 的广泛应用。

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。

2. AT.SIGN 概述

何为 AT.SIGN

AT.Sign 是一种将数字签名特性整合至各类软件应用的新方案。它以软件库的形式提供大量简单易用的接口，通过这些接口，与之整合的应用可请求 AT.Sign 执行数字签名。AT.Sign 还通过高复杂性的、安全的子系统，管理数字签名操作中所用的数字证书。全面的审计日志功能记录了所有的签名操作，可用作检验已签名文档的真实性，从而增强了安全性。

AT.Sign 的主要特性：

- AT.Sign 使用一个安全的证书存储库存储用户的数字证书。这个安全的证书存储库受到强加密保护，而且还可独立安装在其它硬件中。
- 证书存储库的访问受 OTP 认证保护。常用于数字证书存取的是静态密码认证，相比而言，OTP 认证更安全。
- 由于数字证书集中存储在安全的证书存储库中，软件应用可通过网络间接地获取证书以执行数字签名。为了加强访问控制的安全性，这些软件应用在验证用户身份时，通常采用 OTP 认证方案。
- AT.Sign 方案使智能手机和平板电脑等在线设备的用户，通过授权的应用间接地获取证书。在智能手机和平板电脑上存储数字证书，从技术上来说很难实现，即使能实现也不安全。
- 而且，数字证书的获取、数字证书在数字签名中的使用、证书安装、请求事件等操作，都被审计跟踪功能安全地记录下来。审计跟踪还可用作检验已签名文档的真实性，增强了安全性。

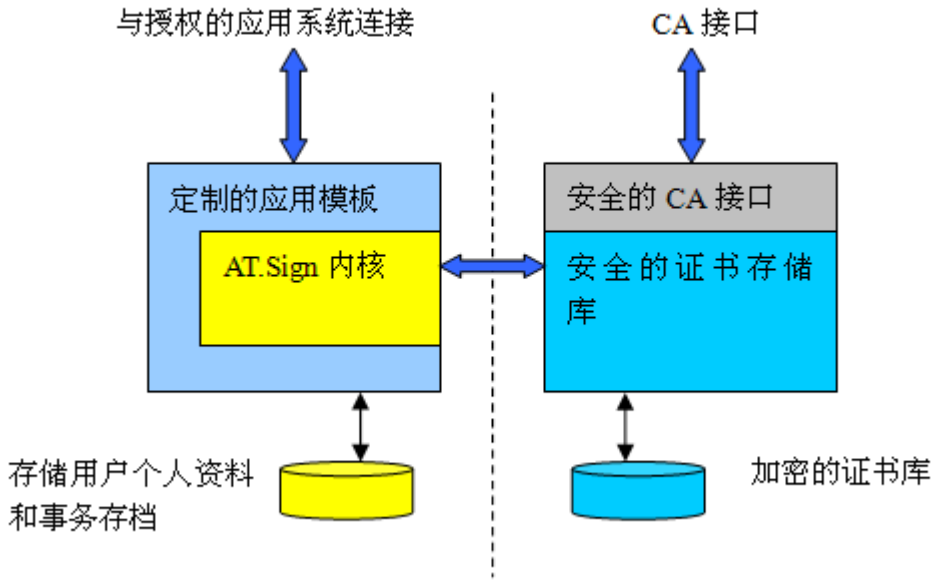
对用户的好处

无论是采用 AT.Sign 实施数字签名的公司，还是将原有的签名系统更换成 AT.Sign 系统的公司，他们都对 AT.Sign 非常满意，并反馈了以下的好处：

增强的安全性	AT.Sign 提供的内置一次性密码（OTP）特性大大改善了证书管理的安全性。而且，AT.Sign 的审计跟踪功能也增强了目标应用系统的安全性。这个审计跟踪功能允许授权用户和系统管理员查看记录，以分析及预防安全性漏洞。
简单灵活的部署	AT.Sign 支持基于 Java 的应用程序接口（API）和 Web Services 的调用。目标应用可轻易地与 AT.Sign 整合，以充分使用 AT.Sign 所提供的功能和特性。
改善的商业进程	由于数字证书是集中存储的，AT.Sign 大大降低了证书的发放、更换和撤销等管理负担和成本。

AT.SIGN 组件

从结构上来说，AT.Sign 包含以下组件（或子系统）：



这些组件的细节如下：

AT.SIGN 内核	• 维护注册用户的个人资料； • 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系统关键事件进行记录和存档； • 提供一个安全接口以查看审计跟踪和存档。
安全的证书存储库	• 为所有的注册用户管理数字证书的安全存储； • 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。

定制的应用模板和接口	• 连接 AT.Sign 服务时，应用系统可采用不同的安全用户认证方式； • 面向应用的 Web Services 接口和 Client Library，使 AT.Sign 与应用系统易于整合； • 提供程序模板，帮助设计师和实施工程师定制符合目标应用的文档标准和工作流程需求。
Web Service API 和 Client Library	• Web Services API 和 Client Library 可用于与目标应用系统的整合； • 根据应用的定制需求，可在 library 中添加要定制的功能。
认证机构（CA）接口	• 实施了一个与 CA 连接的安全渠道（例如，通过这个接口，CA 与 AT.Sign 系统之间可自动完成数字证书的分发）； • 执行 CA 的证书管理指令（例如，撤销，下载黑名单...）；
加密的证书库	• 数字证书被加密存储在硬盘和/或数据库文件中，以防设备和数据被盗或丢失。

3. 常见问题

AT.SIGN 所支持的文档类型

最新版本的 AT.Sign 支持以下文档签署功能：

1. AT.Sign 可签署包含其它文档的摘要的任意格式文件。签署过程是使用数字证书的私玥加密这些文件；
2. AT.Sign 可签署 W3C 标准定义的 XML 文档；
3. AT.Sign 可签署 ISO 32000-1 标准定义的 PDF 文档。

何为证书存储库

我们可以将数字证书存储库比作银行保险库。在银行，各类客户的保险箱被安全地放置在保险库中并受到保护；与此类似，数字证书存储库也维护着众多电子“保险箱”。在数字证书存储库中，每个“保险箱”只属于某一个 AT.Sign 注册用户，并供该用户存放其数字证书。

AT.Sign 允许用户在“保险箱”内存储多个证书，以供用户以不同身份角色使用证书。当用户需要存取这些证书时，AT.Sign 软件的“门警”将通过一次性密码认证方式对其身份进行认证。与大多数 PKI 实施方案中所常见的静态 PIN 码认证相比，一次性密码认证更安全。

数字证书存储库既可连同 AT.Sign 的其它组件安装在单台服务器中，也可独立安装在其它硬件中，以进一步加强整个系统的安全性。

如何将应用整合至 AT.SIGN

我们的工程师将 AT.Sign 设计为“应用引擎”的形式。

这里的“应用引擎”可理解为一组软件服务，这组软件服务可被一系列应用以松耦合的方式调用。“应用引擎”通过对这些应用的一些核心特性和较复杂进程进行因子提取，简化了目标应用的设计、开发和维护。以下是 AT.Sign 应用引擎的一些基本特征：

AT.Sign 应用引擎将数字签名的核心进程和基本服务进行分离。

这些功能（或称为“服务”）采用了底层细节与上层应用分离的实现方式，这种“关注点分离”的方式，清晰地界定了应用引擎的内部和外部，使应用可通过外部的视图调用这些功能。

这些功能足够精确，可重用性高；他们本身也是一个模块，支持“服务自治”；可组合性高，可组合出更复杂的组合功能；互操作性高，可与不同技术的应用协同工作。

AT.Sign 应用引擎提供一组 web service 接口，它专为支持应用实施数字签名而设计。通过这些 web service 接口，使用不同技术和语言开发的应用都可与 AT.Sign 整合。

对于使用 JAVA 开发的应用，AT.Sign 也提供了一组基于 JAVA 的 API 用于整合。通过这些 API, 使用 JAVA 开发的应用可与 AT.Sign 整合。

何为 AT.SIGN 内置的一次性密码技术

内置于 AT.Sign 中的是永泰公司的又一获奖软件解决方案: AT.Pass。

AT.Pass 使用软件令牌生成一次性密码(OTP)。它不但支持令牌分发安装至个人计算机，智能手机，平板电脑和不同类型的移动设备（包括：iOS、安卓和 Windows Mobile 设备），也支持用户根据特别需求申请口令卡。口令卡发送至用户登记的电子邮箱，它包含了一

张预生成的一次性密码列表。指定用户可在有效期限内，按次序使用列表上的一次性密码。

与其它基于硬件令牌的解决方案相比，AT.Pass 大大减轻了部署一次性密码技术的整体成本；因此，在众多场合中，许多应用的用户身份认证都使用了 AT.Pass。

内置的 AT.Pass 版本仅授权于 AT.Sign 的使用。若需要，AT.Pass 亦可作为独立产品授权给用户。许多客户使用它作为基于一次性密码的用户认证解决方案，并将其部署在各种各样的企业在线应用系统之中。