

中华人民共和国烟草行业标准

YC/T 327—2009

烟草行业数字证书应用接口规范

Technical specification for digital certificate application
interface to tobacco industry

2009-12-14 发布

2010-03-01 实施



国家烟草专卖局 发布

目 次

前言	I
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	2
5 烟草行业数字证书格式与发布	3
5.1 烟草行业数字证书结构	3
5.2 烟草行业证书撤销列表结构	3
5.3 烟草行业数字证书特有扩展	4
5.4 烟草行业数字证书 DN 规则	4
5.5 用户证书与应用中身份的关联	5
5.6 烟草行业证书状态发布	5
6 烟草行业数字证书应用接口	6
6.1 烟草行业数字证书应用接口总体框架	6
6.2 安全代理服务	7
6.3 数字签名服务	8
6.4 时间戳服务	9
6.5 在线证书状态服务	10
6.6 目录服务	10
6.7 安全审计服务	10
附录 A (资料性附录) 相关说明	12
A.1 C/S 模式安全通信的实现	12
A.2 单点登录与身份认证	12
附录 B (资料性附录) 数字签名接口和安全审计接口规范	13
B.1 烟草行业证书签名客户端接口	13
B.2 烟草行业证书数字签名服务设备端 Java 接口	17
B.3 烟草行业证书数字签名服务设备 .Net 接口	25
B.4 烟草行业安全审计服务 Java 接口	33

前 言

本标准的附录 A、附录 B 为资料性附录。

本标准由国家烟草专卖局提出。

本标准由全国烟草标准化技术委员会信息分技术委员会(SAC/TC 144/SC 7)归口。

本标准起草单位：国家烟草专卖局烟草经济信息中心。

本标准主要起草人：张雪峰、王海清、刘东平、轩松岭、张萌、王翊心、李伟。

烟草行业数字证书应用接口规范

1 范围

本标准规定了烟草行业数字证书应用的总体框架与应用规范,描述了烟草行业与证书相关应用的技术要求。

本标准适用于烟草行业与数字证书相关应用的规划、设备招标、方案设计以及业务实施。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准,然而,鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本标准。

GB 13000.1—1993 信息技术 通用多八位编码字符集(UCS) 第一部分:体系结构与基本多文种平面(idt ISO/IEC 10646-1:1993)

GB/T 16264.2—2008 信息技术 开放系统互连 目录 第2部分:模型(ISO/IEC 9594-2—2005, IDT)

GB/T 16264.8—2005 信息技术 开放系统互连 目录 第8部分:公钥和属性证书框架(ISO/IEC 9594-8:2001, IDT)

GB/T 19713—2005 信息技术 安全技术 公钥基础设施 在线证书状态协议

GB/T 19771—2005 信息技术 安全技术 公钥基础设施 PKI 组件最小互操作规范

GB/T 20520—2006 信息安全技术 公钥基础设施 时间戳规范

IETF RFC 2251 轻量级目录访问协议(LDAP V3)

IETF RFC 2246 安全传输层协议 V1.0

3 术语和定义

GB/T 16264.2、GB/T 16264.8、GB/T 19713、GB/T 19771、GB/T 20520、GB/T 13000.1 确立的以及下列术语和定义适用于本标准。

3.1

公钥证书 public key certificate

用户的公钥连同其他信息,并由发布该证书的证书认证机构的私钥进行加密使其不可伪造。

[GB/T 16264.8—2005,第3章]。

3.2

证书认证机构 certificate authority; CA

负责创建和分配证书,受用户信任的权威机构。用户可以选择该机构为其创建密钥。

[GB/T 16264.8—2005,第3章]。

3.3

证书撤销列表 certificate revocation list; CRL

一个已标识的列表,它指定了一套证书发布者认为无效的证书。除了普通 CRL 外,还定义了一些特殊的 CRL 类型用于覆盖特殊领域的 CRL。

3.4

注册机构 registration authority; RA

为用户办理证书申请、身份审核、证书下载、证书更新、证书注销以及密钥恢复等实际业务的办事机构或业务受理点。

3.5

目录服务 directory service; DS

分布在网络中的各种节点或服务器提供的分布式数据库服务。

3.6

数字签名 digital signature

允许接收者验证签名人的身份和数据完整性的数据单元。

3.7

时间戳 time stamp

使用数字签名技术产生的数据,签名的对象包括了原始文件的信息、签名参数、签名时间等信息。TSA 对此对象进行数字签名产生时间戳,以证明原始文件在签名时间之前已经存在。

3.8

时间戳机构 time stamp authority; TSA

用来产生和管理时间戳的权威机构。

3.9

数字证书 digital certificate

等同于 3.1 中定义的公钥证书。

3.10

根 CA root CA

是一个特殊的 CA,位于证书认证层次结构的最高层。根 CA 的 CA 证书是自颁发证书。

3.11

安全套接层协议 security socket layer (SSL) protocol

位于网络层协议(如 TCP/IP)和应用程序协议层(如 HTTP)之间的一种安全协议层。它能使客户与服务器应用之间的通信不被攻击者窃听,并且始终对服务器进行认证,还可选择对客户进行认证。

注:SSL 目前最高版本为 3.0。

3.12

安全传输层协议 transport layer security protocol

是在 SSL 版本 3.0 基础上发展而来的一种安全协议,其目的和主要内容与 SSL 3.0 相同。互联网工程任务组 IETF(internet engineering task force)已经将安全传输层协议标准化并正式发布,成为 RFC 2246 标准。

注:安全传输层协议目前的最高版本为 1.0。

4 缩略语

API	应用编程接口
CA	证书认证机构
CDP	CRL 分布点
CRL	证书撤销列表
DN	可辨别名
LDAP	轻量级目录访问协议
OCSP	在线证书状态协议

OID	对象标识符
PKCS	公钥加密标准
PKI	公钥基础设施
RA	注册机构
SSL	安全套接层
SSO	单点登录
TLS	安全传输层协议
TSA	时间戳机构
URI	统一资源标识符
URL	统一资源定位符

5 烟草行业数字证书格式与发布

5.1 烟草行业数字证书结构

烟草行业数字证书结构应符合 GB/T 19771- 2005 中 6.2 定义的证书格式。

证书字段包括：

- a) 版本号 (Version)；
- b) 证书序列号 (Serial Number)；
- c) 颁发者签名算法 (Signature)；
- d) 颁发者可辨别名 (Issuer Name)；
- e) 证书有效时间 (Validity)；
- f) 主体可辨别名 (Subject Name)；
- g) 主体公钥信息 (Subject Public Key Info)；
- h) 证书扩展 (Extensions)；
- i) 权威密钥标识符 (Authority Key Identifier)：
 - 1) 主体密钥标识符 (Subject Key Identifier)；
 - 2) 密钥用法 (Key Usage)；
 - 3) 基本限制 (Basic Constraints)；
 - 4) 扩展密钥用法 (Extended Key Usage)；
 - 5) CRL 分布点 (CRL Distribution Points)。
- j) 颁发者的签名 (Issuer's Signature)。

5.2 烟草行业证书撤销列表结构

烟草行业 CA 通过定期发布证书撤销列表 CRL 来提供证书的状态信息。

烟草行业证书撤销列表结构符合 GB/T 19771—2005 中 6.3 定义的证书撤销列表格式。

证书撤销列表字段包括：

- a) 版本号 (Version)；
- b) 颁发者签名算法 (Signature)；
- c) 颁发者可辨别名 (Issuer Name)；
- d) 本次更新 (This Update)；
- e) 下次更新 (Next Update)；
- f) 撤销的证书 (Revoked Certificates)：
 - 1) 证书序列号 (Certificate Serial Number)；
 - 2) 撤销日期 (Revocation Date)；
 - 3) CRL Entry 扩展 (CRL Entry Extensions)。

- g) CRL 扩展项(CRL Extensions);
- h) 颁发者的签名(Issuer's Signature)。

5.3 烟草行业数字证书特有扩展

烟草行业数字证书中定义了两个特有扩展:证书持有人职务、证书持有人编号。应用系统可根据扩展的 OID 从数字证书中获得对应的证书持有人的职务和编号。编码类型为 GB 13000.1-1993 定义的 UTF8String 格式。这两个扩展只在用户证书中出现。

5.3.1 证书持有人职务扩展定义见表 1。

表 1 证书持有人职务扩展定义

扩展名称	zhiwu
OID	1.3.6.1.4.1.27971.2.1.1
编码类型	UTF8String

5.3.2 证书持有人编号扩展见表 2。

表 2 证书持有人编号扩展定义

扩展名称	bianhao
OID	1.3.6.1.4.1.27971.2.1.2
编码类型	UTF8String

5.4 烟草行业数字证书 DN 规则

烟草行业的证书 DN 包括以下组成部分:

CN(CommonName), OU(OrganizationUnit), O(Organization), C(Country)。

其中的 CN、OU 字段均使用中文, O、C 字段使用英文。编码类型为 GB 13000.1-1993 定义的 UTF8String 格式。任何一个 CN 或 OU 的长度不能超过 50 个汉字或 100 个英文字符、数字。

5.4.1 根 CA DN 规范见表 3。

表 3 根 CA DN 规范定义

CN	O	C
烟草行业根 CA	Tobacco	CN

5.4.2 二级 CA DN 规范见表 4。

表 4 二级 CA DN 规范定义

CN	O	C
国家烟草专卖局 CA	Tobacco	CN
省级 CA		

5.4.3 用户证书 DN 规范见表 5。

表 5 用户证书 DN 规范定义

CN	OU	OU	OU	O	C
姓名 ^a	处名称	司/局名称	国家烟草专卖局	Tobacco	CN
	科名称	处名称	省级单位名称		
	部名称	烟厂名称			
	科名称	市公司名称			
^a 用户的姓名如有重名则应在末尾添加数字以作区分,例如:“CN=某用户 1”。					

5.4.4 服务器证书 DN 规范见表 6。

表 6 服务器证书 DN 规范定义

CN	OU	O	C
服务器域名或 IP	国家烟草专卖局	Tobacco	CN
	省级单位名称		

5.4.5 行业外用户证书 DN 规范见表 7。

表 7 行业外用户证书 DN 规范定义

CN	OU	OU	OU	O	C
姓名 ^a	单位全称	行业外	国家烟草专卖局	Tobacco	CN
	单位全称	行业外	省级单位名称		
^a 用户的姓名如有重名则应在末尾添加数字以作区分,例如:“CN=某用户 1”。					

5.5 用户证书与应用中身份的关联

用户的数字证书是其身份的标识,用户在各个应用中的身份(用户名)应与该用户的数字证书进行关联,宜使用数字证书中的 DN 作为关联的首选要素。

5.6 烟草行业证书状态发布

当发现数字证书遗失或私钥失密时,证书持有者应向烟草行业 CA 提出证书注销申请,CA 系统经过审核后将实施证书注销并发布该证书的废止状态,应用系统可通过 CRL 或 OCSP 两种模式进行证书状态查询。

5.6.1 CRL 模式

烟草行业 CA 系统通过二级 CA 系统(国家局 CA 和省级 CA)定时发布本系统 CRL 到内网区主目录服务器上,通过目录服务器复制协议将主目录服务器上的数据复制到公共访问区的从目录服务器。应用系统通过 RFC 2251 定义的轻量级目录访问协议(LDAP V3)访问公共区域的从目录服务器来获取最新的 CRL,进行证书有效性判断。CRL 模式的实现如图 1 所示。



图 1 CRL 模式示意图

5.6.2 OCSP 模式

烟草行业 CA 系统在二级 CA 系统(国家烟草专卖局 CA 和省级 CA)区域提供 OCSP 服务,应用系统通过 GB/T 19713-2005 定义的在线证书状态协议访问 OCSP 服务器,查询证书状态。OCSP 模式的实现如图 2 所示。



图 2 OCSP 模式示意图

6 烟草行业数字证书应用接口

6.1 烟草行业数字证书应用接口总体框架

烟草行业数字证书应用接口由数字证书应用的 6 个相关服务模块构成。

烟草行业数字证书应用支撑平台提供了烟草行业数字证书应用的 3 个基础服务：安全代理服务，数字签名服务，时间戳服务。烟草行业数字证书签发服务平台提供了烟草行业数字证书应用的 3 个辅助性服务：目录服务，在线证书状态服务，安全审计服务。其中目录服务和在线证书状态服务是由应用系统通过标准接口进行访问，无需另行建设。烟草行业数字证书应用接口总体框架如图 3 所示。

鉴于 C/S 模式安全通信和单点登录系统的复杂性，本标准不对这两类安全功能的实现作出强制性要求，相关说明见附录 A。

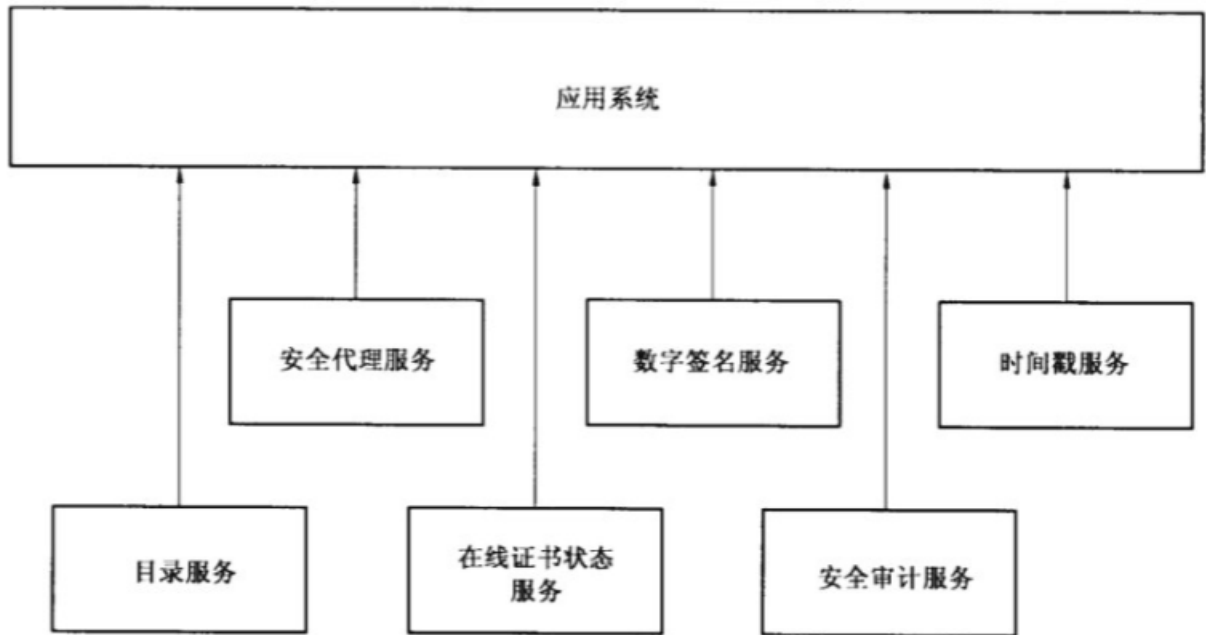


图 3 烟草行业数字证书应用接口总体框架示意图

6.1.1 安全代理服务

安全代理服务应用提供基于数字证书的可靠身份认证和数据加密传输的安全服务，宜实现身份认证和机密性的安全需求。安全代理服务通过部署 SSL 安全代理服务设备来构建。

6.1.2 数字签名服务

数字签名服务为应用提供针对特定数据内容的数字签名和验证服务。宜实现数据的完整性和不可否认性安全需求。数字签名服务通过部署数字签名服务设备以及在应用中部署其相关 API 来构建。

6.1.3 时间戳服务

时间戳机构给用户提供的颁发时间戳服务,由用户提供文件或数据,时间戳机构给此文件或数据签发时间戳。时间戳服务的功能是提供可靠的时间信息证据,以证明某个信息在某个时间(或以前)的存在,或证明某个操作发生的时间,宜实现数字信息与可信时间的不可伪造的捆绑。时间戳服务通过部署时间戳服务设备以及在应用中部署其相关 API 来构建。

6.1.4 目录服务

应用系统可从目录服务器中查询或者获取到任何公开的证书,并可通过该服务获取由 CA 发布的,最新的证书撤销列表 CRL 文件,从而实现证书状态的检查。

6.1.5 在线证书状态服务

应用系统可通过在线证书状态协议实时查询证书的状态。

6.1.6 安全审计服务

安全审计服务提供应用安全审计日志的收集和分析工作,应用在进行数字证书相关操作的时候,通过安全审计服务接口将审计日志报送至安全审计服务。

6.2 安全代理服务

6.2.1 安全代理服务的实现

安全代理服务通过部署 SSL 安全代理服务设备来实现。

SSL 安全代理服务设备部署在客户端(浏览器)与后台的应用服务器之间,起到了对应用服务器的反向代理作用,有效地保护了应用服务器。用户的浏览器与 SSL 安全代理服务设备之间使用数字证书进行可靠的身份认证,并建立加密的通道,来自用户的访问通过 SSL 安全代理服务设备安全地到达后台的应用服务器。SSL 安全代理服务设备根据配置,向后台的应用服务器传递用户证书的信息。

安全代理服务的实现如图 4 所示。

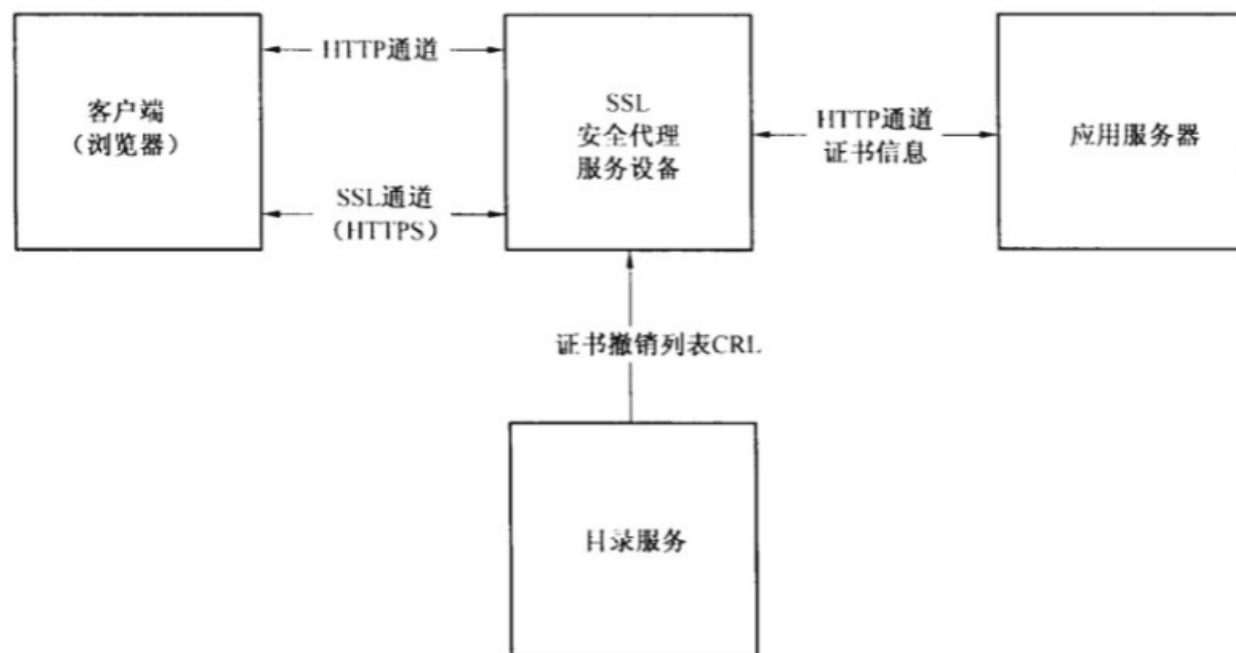


图 4 SSL 安全代理服务应用示意图

SSL 安全代理服务设备应进行如下配置：

- 为 SSL 安全代理服务设备申请服务器证书。从 SSL 安全代理服务设备属地的 CA 中心申请服务器证书,服务器证书 DN 中的 CN 应是域名或 SSL 安全代理服务设备的 IP 地址。
- 将请求客户端证书配置为强制方式,即必须提供客户端证书;并应配置颁发客户端证书的 CA 的根证书以建立进行客户端证书验证时的 CA 信任域。如果应用需要获得建立 SSL 连接的客户端证书信息,还应配置向应用服务器传递证书信息的方式和参数。

- c) 在 SSL 安全代理服务设备 CA 信任域配置 CA 根证书。
- d) 为 SSL 安全代理服务设备进行网络配置。SSL 安全代理服务设备对外提供服务的 IP 地址就是原来应用服务器对外提供服务的 IP 地址,域名对应的也是这个 IP 地址。SSL 安全代理服务设备使用 443 端口提供 SSL 服务,防火墙上要允许来自外部的 443 端口访问。
- e) 配置 SSL 安全代理服务设备的访问控制列表,设定必须通过 SSL 以及客户证书认证才能访问的资源列表。
- f) 配置下载 CRL 所需的 CA 中心的 LDAP 目录服务的 IP 地址和服务端口,确保 SSL 安全代理服务设备能够获得 CA 发布的 CRL。
- g) 配置后台需要代理的应用服务器地址和端口,使之能够转发客户端的请求报文。

SSL 安全代理服务设备可为多个应用提供共享的安全服务。在多个应用需要不同的外部域名或 IP 时,应在 SSL 安全代理服务设备内部配置针对每个域名或 IP 的 SSL 服务器证书。

6.2.2 安全代理服务应用接口

SSL 安全代理服务设备将根据配置,将用户数字证书的域值作为一个字符串加入 HTTP URL 参数或 HTTP HEADER 参数并向应用服务器传递。

后传证书信息包括:

- a) 主体可辨别名(Subject Name);
- b) 颁发者可辨别名(Issuer Name);
- c) 证书序列号(Serial Number);
- d) 证书有效时间(Validity)。

应用服务器从 HTTP URL 或 HTTP HEADER 中获取 SSL 安全代理服务设备传递来的用户证书信息,进行用户身份认证,判断用户的身份信息,确认用户数字证书的有效期,从而进行后续的访问权限判断、证书有效期人机提示和日志记录。

6.3 数字签名服务

6.3.1 数字签名服务的实现

数字签名服务通过部署数字签名服务设备,数字签名服务设备 API 和数字签名客户端 API 来实现。

数字签名客户端 API 供应用客户端调用;数字签名服务设备 API 供应用服务器调用,负责将应用中接收到的签名数据发送到数字签名服务设备中,并接收数字签名服务设备的验证结果返回给应用;数字签名服务设备接收签名 API 发送的签名数据,对签名数据和签名证书进行有效性验证,并返回验证结果。数字签名服务的实现如图 5 所示。

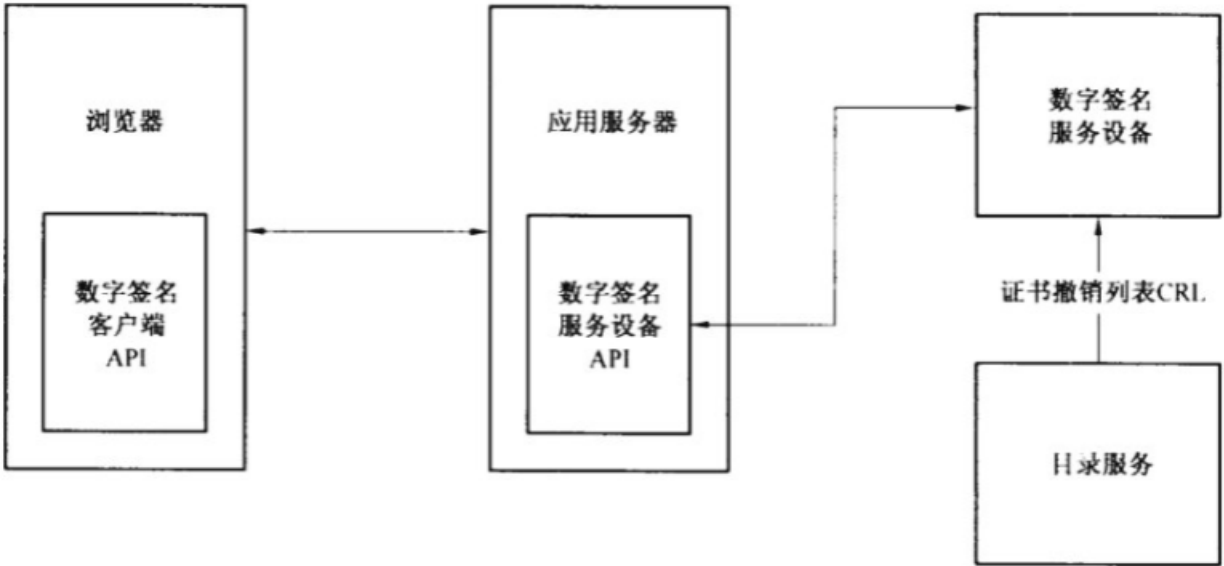


图 5 数字签名服务应用示意图

数字签名服务应进行如下配置：

- a) 数字签名服务设备需和应用服务器部署需保持网络连通,确保应用服务器中部署的数字签名服务设备 API 能够通过网络访问到数字签名服务设备;
- b) 在数字签名服务设备 CA 信任域配置 CA 的根证书;
- c) 如果需要服务器端签名,则要为数字签名服务设备申请服务器签名证书;
- d) 配置下载 CRL 所需的 CA 中心的 LDAP 目录服务的 IP 地址和服务端口,确保数字签名服务设备能够获得 CA 发布的 CRL。

6.3.2 数字签名服务应用接口

数字签名服务提供客户端 API 和服务端 API(包括 Java 和 .Net 接口)。在 Web 应用结构中,数字签名客户端 API 以 ActiveX 控件方式提供,供浏览器页面调用。对于有不可否认性(或称为留痕)需求的应用,宜建立签名库,签名库中保留了以往所有的签名数据,供需要时提取验证。

数字签名接口的具体调用方式参见附录 B。

为了保证对多种文字编码的支持,宜在调用客户端签名之前,将原文统一转换成 UTF8 编码然后进行后续的签名处理。

6.4 时间戳服务

6.4.1 时间戳服务的实现

时间戳服务通过部署时间戳服务设备及其 API 来实现。

时间戳服务设备 API 供应用服务端调用,应用服务器向时间戳服务设备申请时间戳,时间戳服务设备根据请求的内容和当前时间生成时间戳。时间戳服务的应用如图 6 所示。

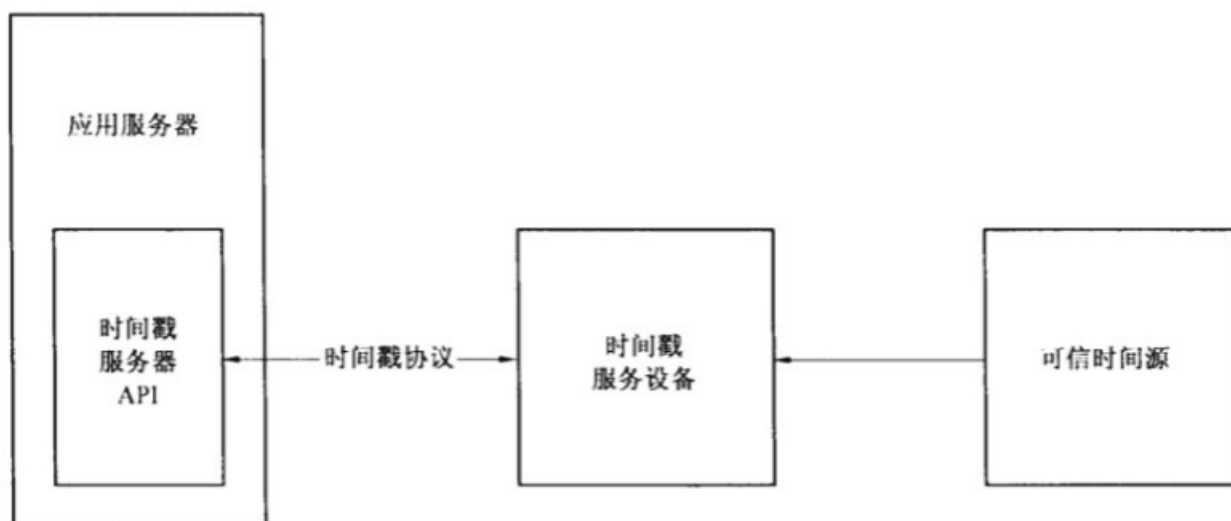


图 6 时间戳服务应用示意图

时间戳服务应进行如下配置：

- a) 时间戳服务设备是一个网络设备,和应用服务器部署在同一网段,配置网络使得时间戳服务设备 API 能够通过网络访问到时间戳服务设备;
- b) 配置时间戳服务设备能够连接到可信时间源,可信时间源宜使用国家授时中心发布的可信时间(需要专用的授时接收设备)或从网络上通过 NTP 获得可信时间;
- c) 从属地 CA 中心申请时间戳服务设备证书并配置到时间戳服务设备,该证书用来签发时间戳。

6.4.2 时间戳服务应用接口

应用服务器通过调用时间戳 API 来访问时间戳服务设备。时间戳服务设备支持 GB/T 20520 - 2006 定义的时间戳协议。

6.5 在线证书状态服务

6.5.1 在线证书状态服务的实现

在线证书状态服务是烟草行业数字证书签发服务平台的组成部分,应用系统无需另行建设。在线证书状态 API 由应用系统调用,与在线证书状态服务进行通信。在线证书状态服务的实现如图 7 所示。

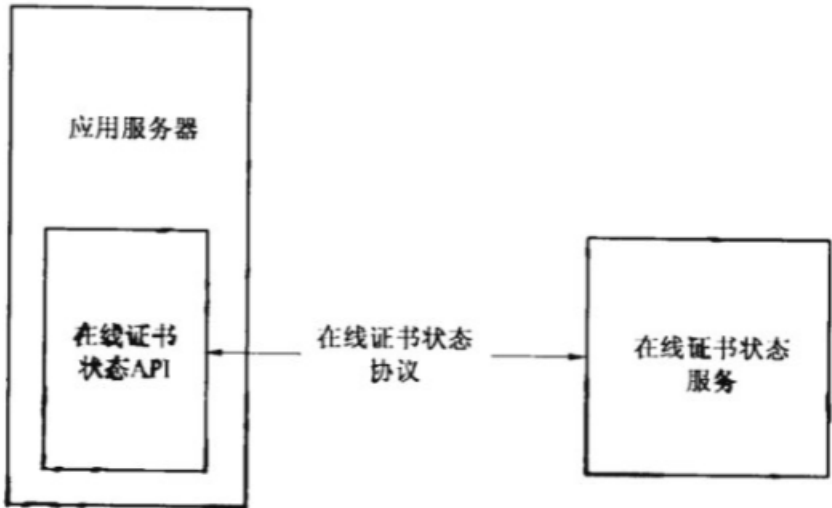


图 7 在线证书状态服务应用示意图

6.5.2 在线证书状态服务应用接口

应用服务器通过调用在线证书状态 API 来访问在线证书状态服务。在线证书状态服务支持 GB/T 19713 2005 定义的在线证书状态协议。

6.6 目录服务

6.6.1 目录服务的实现

目录服务的实现如图 8 所示。



图 8 目录服务应用示意图

6.6.2 目录服务应用接口

应用服务器通过 RFC 2251 定义的轻量级目录访问协议(LDAP V3)访问目录服务。

6.6.3 烟草行业数字证书与证书撤销列表 CRL 发布

烟草行业 CA 系统将本系统数字证书和 CRL 发布到目录服务器上,应用系统应通过轻量级目录访问协议(LDAP V3)访问,并获取目录中存储的数字证书和 CRL。

烟草行业 CA 系统根据每个数字证书 DN 在目录服务器上创建一个对应的目录服务器条目对象,数字证书值在该证书 DN 对应的对象下的 userCertificate 属性中。

烟草行业 CA 系统使用“CRL 分布点”技术来发布 CRL。多个证书共享一个 CRL 分布点,CRL 发布采用 DIR 模式,CRL 值在 CDP 对应的对象下的 CertificateRevocationList 属性中。

6.7 安全审计服务

6.7.1 安全审计服务的实现

数字证书用户在通过数字证书进行身份认证、登录、登出应用系统时,应用系统应将安全审计日志

报送至安全审计服务,安全审计服务将审计日志集中存储在其自身的安全审计日志仓库中。安全审计服务应用示意图见图 9。

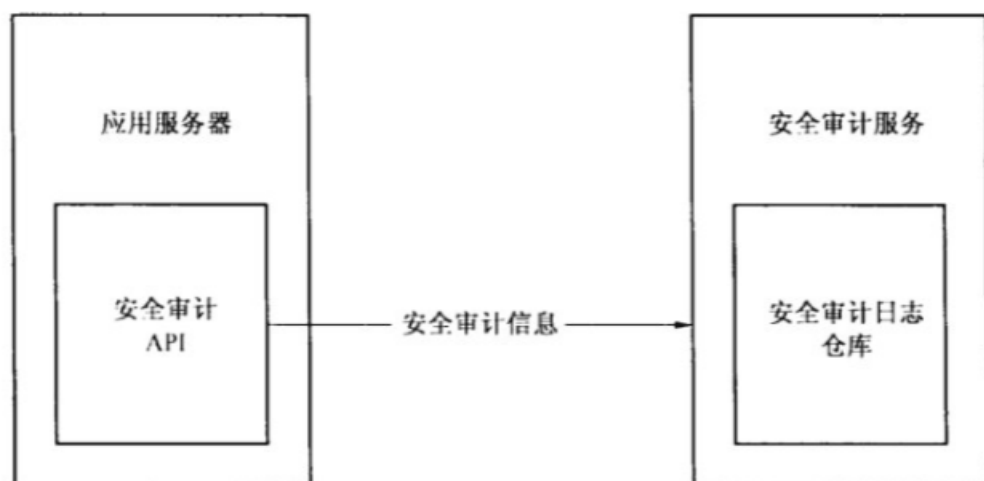


图 9 安全审计服务应用示意图

6.7.2 安全审计日志内容

安全审计日志包括:

- a) 用户认证日志:证书用户 DN、认证时间、认证系统 ID、认证结果;
- b) 用户登录日志:用户 ID、登录时间、业务系统 ID、登录结果;
- c) 用户登出日志:用户 ID、登出时间、业务系统 ID、登出结果。

6.7.3 安全审计服务应用接口

应用服务器通过调用安全审计 API 来访问安全审计服务,接口定义参见附录 B。

附 录 A
(资料性附录)
相 关 说 明

A.1 C/S 模式安全通信的实现

鉴于 C/S 应用的种类和协议情况复杂,本标准暂不强制规定 C/S 架构下实现安全通信的具体方法。

C/S 应用实现安全通信,可根据具体情况采用以下的方案:

- a) 在服务器端部署安全代理设备;对客户端应用程序进行修改,调用 SSL API,实现与服务器端安全代理设备的安全连接与认证。
- b) 在服务器端部署安全代理设备;在客户端部署 SSL 客户端代理,应用程序修改网络连接配置,通过 SSL 客户端代理转发实现与服务器端安全代理设备的安全连接与认证。
- c) 在服务器端部署 SSL VPN 设备,客户端在访问 SSL VPN 设备并认证之后,应用程序通过 SSL VPN 的安全通道访问服务器。

A.2 单点登录与身份认证

单点登录系统与数字证书之间的关系比较松散,考虑到单点登录系统面向的应用场景以及实现方式的复杂性,本标准不对单点登录系统进行描述。

单点登录系统宜使用安全代理服务(SSL 协议)实现基于数字证书的身份认证。如果使用非 SSL 协议的身份认证系统,则该身份认证系统应支持规范中定义的烟草行业数字证书相关规范。

附录 B

(资料性附录)

数字签名接口和安全审计接口规范

B.1 烟草行业证书签名客户端接口

B.1.1 数据类型说明

BSTR(Basic String)是微软公司(Microsoft)MSDN 中定义的一种数据类型。

B.1.2 获取控件版本信息

接口名称: BSTR getVersion()
 功能简介: 获取客户端签名控件版本
 参数说明: 无
 返回值: BSTR 版本号和 Build 号

B.1.3 设置对原文的编码

接口名称: public void NSSetCodePage(DWORD codepage)
 功能简介: 设置对原文的编码
 参数说明: DWORD codepage: 编码 OID
 常用的编码 OID 值:
 UTF8 65001(本标准建议)
 GBK 936
 如果不设置,将使用用户系统的默认编码,不作转码。
 返回值: 无(调用本接口完成后,应调用“B.1.25 获得错误号”接口来判断是否正常完成。
 如果验签名正常,该接口的返回值应该为 0。)

B.1.4 Detached 方式签名

接口名称: BSTR NSDetachedSign(BSTR plainText, BSTR deSignerDN)
 功能简介: 对输入的原文做 detached 方式签名,再将签名的结果做 Base64 编码,并返回编码结果
 参数说明: BSTR plainText 原文
 BSTR deSignerDN 签名证书 DN
 返回值: BSTR BASE64 编码后的签名

B.1.5 Detached 方式验签名

接口名称: Void NSDetachedVerify(BSTR signedMsg, BSTR plainText)
 功能简介: 对输入的签名先作 Base64 解码、验签,同时校验签名证书的签名、有效期、证书链的有效性以及 CRL
 参数说明: BSTR signedMsg Base64 编码的签名
 BSTR plainText 原文
 返回值: 无(调用本接口完成后,应调用“B.1.25 获得错误号”接口来判断是否正常完成。如果验签名正常,该接口的返回值应该为 0。)

B.1.6 Attached 方式签名

接口名称: BSTR NSAttachedSign(BSTR deSignerDN)
 功能简介: 对输入的原文做 attached 方式签名,再将签名的结果做 Base64 编码,并返回编码结果

参数说明: BSTR deSignerDN 签名证书主题

返回值: Base64 编码的签名包

B. 1.7 Attached 方式验签名

接口名称: Void NSAttachedVerify(BSTR signedMsg)

功能简介: 对输入的签名先做 Base64 解码、验签,同时校验签名证书的签名、有效期、证书链的有效性以及 CRL

参数说明: BSTR signedMsg Base64 格式的签名包

返回值: 无(调用本接口完成后,应调用“B. 1.25 获得错误号”接口来判断是否正常完成。如果验签名正常,该接口的返回值应该为 0。)

B. 1.8 RAW 方式签名

接口名称: BSTR NSRawSign(BSTR deSignerDN)

功能简介: 对输入的原文做 RAW 方式签名,再将签名的结果做 Base64 编码,并返回编码结果

参数说明: BSTR deSignerDN 签名证书主题

返回值: BSTR Base64 编码的签名包

B. 1.9 RAW 方式验签名

接口名称: Void NSRawVerify(BSTR signedMsg, BSTR deSignerDN, BSTR plainText)

功能简介: 对输入的签名先做 Base64 解码、验签,同时校验签名证书的签名、有效期、证书链的有效性以及 CRL

参数说明: BSTR signedMsg Base64 格式的签名包

BSTR deSignerDN 签名证书主题

BSTR plainText 原文

返回值: 无(调用本接口完成后,应调用“B. 1.25 获得错误号”接口来判断是否正常完成。如果验签名正常,该接口的返回值应该为 0。)

B. 1.10 使用证书颁发者和证书序列号选择证书进行 Attached 方式签名

接口名称: BSTR NSAttachedSignByIssuerSN(BSTR deSignerSN, BSTR IssuerDN)

功能简介: 对输入的原文做 attached 方式签名,再将签名的结果做 Base64 编码,并返回编码结果

参数说明: BSTR deSignerSN 签名证书序列号

BSTR IssuerDN 签名证书颁发者

返回值: BSTR Base64 编码的签名包

B. 1.11 使用证书颁发者和证书序列号选择证书进行 Detached 方式签名

接口名称: BSTR NSDetachedSignByIssuerSN(BSTR plaintext, BSTR deSignerSN, BSTR IssuerDN)

功能简介: 对输入的原文做 detached 方式签名,再将签名的结果做 Base64 编码,并返回编码结果

参数说明: BSTR plainttext 原文

BSTR deSignerSN 签名证书序列号

BSTR IssuerDN 签名证书颁发者

返回值: BSTR BASE64 编码后的签名

B. 1.12 事后验签

接口名称: Void NSAfterwardsVerify(BSTR signedMsg)

功能简介: 对输入的签名先做 Base64 解码、验签

参数说明: BSTR signedMsg Base64 格式的签名包

返回值： 无(调用本接口完成后,应调用“B. 1. 25 获得错误号”接口来判断是否正常完成。如果验签名正常,该接口的返回值应该为 0。)

B. 1. 13 加入一个文件

接口名称： Void NSAddFile(BSTR fileName)

功能简介： 产生的数据是签名或加密操作的输入数据

参数说明： BSTR fileName 带路径的文件名

返回值： 无(调用本接口完成后,应调用“B. 1. 25 获得错误号”接口来判断是否正常完成。如果验签名正常,该接口的返回值应该为 0。)

B. 1. 14 加入一个表单项

接口名称： Void NSAddFormItem(BSTR itemContent)

功能简介： 产生的数据是签名或加密操作的输入数据

参数说明： BSTR itemContent 表单内容

返回值： 无(调用本接口完成后,应调用“B. 1. 25 获得错误号”接口来判断是否正常完成。如果验签名正常,该接口的返回值应该为 0。)

B. 1. 15 直接设定原文

接口名称： Void NSSetPlainText(BSTR plaintext)

功能简介： 产生的数据是签名或加密操作的输入数据

参数说明： BSTR plaintext 原文

返回值： 无(调用本接口完成后,应调用“B. 1. 25 获得错误号”接口来判断是否正常完成。如果验签名正常,该接口的返回值应该为 0。)

B. 1. 16 得到一个文件

接口名称： BSTR NSGetFile()

功能简介： 验签成功后,获取签名包中的文件

参数说明： 无

返回值： BSTR 如果返回“”代表已经没有文件数据,否则返回文件名

B. 1. 17 得到一个表单项

接口名称： BSTR NSGetFormItem()

功能简介： 验签成功后,获取签名包中的表单项

参数说明： 无

返回值： BSTR 返回一个表单项的内容

B. 1. 18 直接得到原文

接口名称： BSTR NSGetPlainText()

功能简介： 验签成功后,获取签名包中的原文

参数说明： 无

返回值： BSTR 原文

B. 1. 19 制作数字信封

接口名称： BSTR NSEncryptedEnvelop(BSTR deReceiptDN)

功能简介： 对输入的原文做数字信封,再做 Base64 编码,返回编码结果

参数说明： BSTR deReceiptDN 默认的加密证书的主题

返回值： BSTR 返回数字信封的 Base64 编码结果

B. 1. 20 解数字信封

接口名称： Void NSDecryptedEnvelop(BSTR envelopedMsg)

功能简介： 对输入的数字信封先做 Base64 解码,然后解密该数字信封

参数说明: BSTR envelopedMsg Base64 编码的数字信封
 返回值: 无(调用本接口完成后,应调用“B. 1. 25 获得错误号”接口来判断是否正常完成。如果验签名正常,该接口的返回值应该为 0。)

B. 1. 21 制作带签名的数字信封

接口名称: BSTR NSSignedAndEncryptedEnvelop(BSTR deSignerDN, BSTR deReciptDN)
 功能简介: 对输入的原文做 attached 方式签名的数字信封,再将该数字信封做 Base64 编码并返回编码结果
 参数说明: BSTR deSignerDN 默认的签名者的证书主题
 BSTR deReciptDN 默认的接收者的证书主题
 返回值: BSTR Base64 编码的带签名的数字信封

B. 1. 22 解带签名的数字信封并验证

接口名称: Void NSDecryptedAndVerifiedEnvelop(BSTR signedAndEnvelopedMsg)
 功能简介: 对输入的带签名的数字信封先做 Base64 解码,然后解密并验证该数字信封,同时校验签名证书的签名、有效期、证书链的有效性以及 CRL
 参数说明: BSTR signedAndEnvelopedMsg Base64 编码过的带签名的数字信封
 返回值: 无(调用本接口完成后,应调用“B. 1. 25 获得错误号”接口来判断是否正常完成。如果验签名正常,该接口的返回值应该为 0。)

B. 1. 23 获得签名证书信息

接口名称: BSTR NSGetSignerCertInfo(DWORD type)
 功能简介: 获取签名证书信息
 参数说明: DWORD type 一个整数,用来指出需要获得的证书内容
 当 type = 1 时,代表证书主题 DN
 当 type = 2 时,代表证书颁发者 DN
 当 type = 3 时,代表证书有效期起始时间
 当 type = 4 时,代表证书有效期终止时间
 当 type = 5 时,代表证书序列号
 返回值: BSTR 与 type 匹配的证书内容

B. 1. 24 获得加密证书信息

接口名称: BSTR NSGetReciptCertInfo(DWORD type)
 功能简介: 获取加密证书信息
 参数说明: DWORD type 一个整数,用来指出需要获得的证书内容
 当 type = 1 时,代表证书主题 DN
 当 type = 2 时,代表证书颁发者 DN
 当 type = 3 时,代表证书有效期起始时间
 当 type = 4 时,代表证书有效期终止时间
 当 type = 5 时,代表证书序列号
 返回值: BSTR 与 type 匹配的证书内容

B. 1. 25 获得错误号

接口名称: long errorNum()
 功能简介: 获得错误号。
 签名控件功能调用后应检查此接口,判断调用是否成功。详细错误号定义见后面的详细描述。
 参数说明: 无

返回值: long 错误号

B.1.26 获得错误信息

接口名称: BSTR errMsg()

功能简介: 获得错误信息

参数说明: 无

返回值: BSTR 错误信息

B.1.27 获得系统错误号

接口名称: long errorCode()

功能简介: 获得系统错误号。

如果调用 errorNum()返回的错误在错误列表中不能查到,则应该使用此接口获得进一步的错误号。

参数说明: 无

返回值: long 系统错误号

B.1.28 错误代码

错误码	错误内容
—100000	没有可用内存
· 100001	输入参数为空
—100002	Base64 解码失败
· 100003	Base64 编码失败
—100005	用户取消
· 100010	找不到证书
· 100011	缺少数据
· 100020	数据类型错误
—100021	消息类型错误
· 100022	消息错误
—100023	证书的签名错误
—100024	证书过期
—100025	证书已废止
—100026	证书不可信任
—100027	上级证书未发现
100028	没有找到匹配私钥
· 100029	证书解析错误
—100030	证书签名非法
· 100031	打开证书存储区错误
100032	获得 CSP 失败
—100033	签名失败

B.2 烟草行业证书数字签名服务设备端 Java 接口

B.2.1 概述

数字签名服务 Java 接口提供如下的类供应用使用:

类名	说明
NetSignAgent	数字签名系统客户端接口主类

NetSignResult	数字签名系统客户端结果类
NetSignAgentException	数字签名系统客户端异常
ServerProcessException	数字签名系统服务器端异常

B.2.2 NetSignAgent 类

B.2.2.1 获取版本

接口名称:	public static String getVersion()
功能简介:	获取版本号
参数说明:	无
返回值:	String: 版本信息
异常:	无

B.2.2.2 初始化 NetSignAgent

接口名称:	public static void initialize()
功能简介:	使用当前类路径中的 netsignagent.properties 文件中的配置, 初始化签名服务器
参数说明:	无
返回值:	无
异常:	NetSignAgentException 配置文件中初始化的项不足或者错误, 则抛出此异常

B.2.2.3 Attached 签名

接口名称:	public static NetSignResult attachedSignature(byte[] plainText, java.lang.String subject, java.lang.String digestAlg, boolean useTSA)
功能简介:	对输入的原文做 attached 方式签名, 再将签名的结果做 Base64 编码, 并返回编码结果
参数说明:	plainText 原文 subject 用于签名的私钥对应的公钥证书的主题 digestAlg 摘要算法 useTSA 是否请求 TSA 服务
返回值:	NetSignResult, 其中包含: Base64 后的签名结果 Base64 后的时间戳
异常:	NetSignAgentException 客户端异常 ServerProcessException 服务器端异常

B.2.2.4 Attached 方式验签名

接口名称:	public static NetSignResult attachedVerify(java.lang.String signedText, java.lang.String tsaText, boolean needCert)
功能简介:	对输入的签名先做 Base64 解码、验签, 同时校验签名证书的签名、有效期、证书链的有效性以及 CRL
参数说明:	signedText—签名数据 tsaText—时间戳, 如果该参数的值是 null, 表示不用验证时间戳 needCert—标明是否返回用于验证签名的公钥证书
返回值:	NetSignResult, 其中包含: byte[] 类型的原文 String 类型的时间戳生成时间 String 类型的证书主题

String 类型的证书序列
 String 类型的证书颁发者主题
 String 类型的证书有效期起始时间
 String 类型的证书有效期终止时间
 异常: NetSignAgentException 客户端异常
 ServerProcessException 服务器端异常

B.2.2.5 Detached 签名

接口名称: public static NetSignResult detachedSignature(byte[] plainText, String subject, String digestAlg, boolean useTSA)
 功能简介: 对输入的原文做 detached 方式签名, 再将签名的结果做 Base64 编码, 并返回编码结果
 参数说明: plainText—原文
 subject 用于签名的私钥对应的公钥证书的主题
 digestAlg 摘要算法
 useTSA 是否请求 TSA 服务
 返回值: NetSignResult, 其中包含:
 Base64 后的签名结果
 Base64 后的时间戳
 异常: NetSignAgentException 客户端异常
 NetSignServerException 服务器端异常

B.2.2.6 Detached 方式验签名

接口名称: public static NetSignResult detachedVerify(byte[] plainText, String signedText, String tsaText, boolean needCert)
 功能简介: 对输入的签名先做 Base64 解码、验签, 同时校验签名证书的签名、有效期、证书链的有效性以及 CRL
 参数说明: plainText—原文
 signedText—签名数据
 tsaText 时间戳, 如果该参数的值是 null, 表示不用验证时间戳
 needCert 标明是否返回用于验证签名的公钥证书
 返回值: NetSignResult, 其中包含:
 byte[] 类型的原文
 String 类型的时间戳生成时间
 String 类型的证书主题
 String 类型的证书序列
 String 类型的证书颁发者主题
 String 类型的证书有效期起始时间
 String 类型的证书有效期终止时间
 异常: NetSignAgentException 客户端异常
 ServerProcessException 服务器端异常

B.2.2.7 制作数字信封

接口名称: public static NetSignResult makeEnvelope(byte[] plainText, String subject, String sAlg)
 功能简介: 对输入的原文做数字信封, 再做 Base64 编码, 返回编码结果

参数说明: plainText—原文
 subject—用于 RSA 加密的公钥证书的主题
 sAlg—用于对成加密的对称算法

返回值: NetSignResult, 其中包含:
 Base64 后的数字信封

异常: NetSignAgentException 客户端异常
 NetSignServerException 服务器端异常

B.2.2.8 制作带签名的数字信封

接口名称: public static NetSignResult makeMSEnvelope(byte[] plainText, String signSubject, String encSubject, String digestAlg, String sAlg)

功能简介: 对输入的原文做 attached 方式签名的数字信封, 再将该数字信封作 Base64 编码并返回编码结果

参数说明: plainText—原文
 signSubject—用于签名的私钥对应的公钥证书的主题
 encSubject—用于 RSA 加密的公钥证书的主题
 digestAlg—摘要算法
 sAlg—用于对成加密的对称算法

返回值: NetSignResult, 其中包含:
 Base64 后的数字信封

异常: NetSignAgentException 客户端异常
 ServerProcessException 服务器端异常

B.2.2.9 解数字信封

接口名称: public static NetSignResult decryptEnvelope(String encText, String subject)

功能简介: 解数字信封

参数说明: encText—数字信封
 subject—用于解密数字信封的私钥对应的公钥证书的主题

返回值: NetSignResult, 其中包含:
 byte[] 类型的原文
 String 类型的证书主题
 String 类型的证书序列号
 String 类型的证书颁发者主题
 String 类型的证书有效期起始时间
 String 类型的证书有效期终止时间

异常: NetSignAgentException 客户端异常
 ServerProcessException 服务器端异常

B.2.2.10 解带签名的数字信封并验证

接口名称: public static NetSignResult decryptMSEnvelope(String encText, String subject)

功能简介: 对输入的带签名的数字信封先做 Base64 解码, 然后解密并验证该数字信封, 同时校验签名证书的签名、有效期、证书链的有效性以及 CRL

参数说明: encText—数字信封
 subject—用于解密数字信封的私钥对应的公钥证书的主题

返回值: NetSignResult, 其中包含:
 byte[] 类型的原文

String 类型的签名证书主题
 String 类型的签名证书序列
 String 类型的签名证书颁发者主题
 String 类型的签名证书有效期起始时间
 String 类型的签名证书有效期终止时间
 String 类型的加密证书主题
 String 类型的加密证书序列号
 String 类型的加密证书颁发者主题
 String 类型的加密证书有效期起始时间
 String 类型的加密证书有效期终止时间
 异常: NetSignAgentException 客户端异常
 NetSignServerException 服务器端异常

B.2.2.11 RAW 签名

接口名称: `public static NetSignResult rawSignature(byte[] plainText, String subject, boolean useTSA)`
 功能简介: 对输入的原文做 RAW 方式签名, 再将签名的结果做 Base64 编码, 并返回编码结果
 参数说明: plainText—原文
 subject—用于签名的私钥对应的公钥证书的主题
 useTSA—是否请求 TSA 服务
 返回值: NetSignResult, 其中包含:
 Base64 后的签名结果
 Base64 后的时间戳
 异常: NetSignAgentException 客户端异常
 ServerProcessException 服务器端异常

B.2.2.12 RAW 方式验签名

接口名称: `public static NetSignResult rawVerify(byte[] plainText, String signedText, String tsaText, X509Certificate cert)`
 功能简介: 对输入的签名先做 Base64 解码、验签, 同时校验签名证书的签名、有效期、证书链的有效性以及 CRL
 参数说明: plainText—原文
 signedText—签名结果
 tsaText 时间戳, 如果该参数的值是 null, 表示不用验证时间戳
 cert 用于验签名的证书
 返回值: NetSignResult, 其中包含:
 byte[] 类型的原文
 String 类型的时间戳生成时间
 String 类型的证书主题
 String 类型的证书序列
 String 类型的证书颁发者主题
 String 类型的证书有效期起始时间
 String 类型的证书有效期终止时间
 异常: NetSignAgentException 客户端异常
 NetSignServerException 服务器端异常

B.2.3 NetSignResult 类**B.2.3.1 常量定义**

类名	说明
SIGN_TEXT	签名数据
PLAIN_TEXT	明文数据
ENC_TEXT	数字信封数据
TSA_TEXT	时间戳数据
SIGN_CERT	签名证书
TSA_GEN_TIME	时间戳生成时间
SIGN_SUBJECT	签名证书主题
SIGN_SER_NUMBER	签名证书序列号
SIGN_ISSUER_SUBJECT	签名证书颁发者
SIGN_START_TIME	签名证书生效时间
SIGN_END_TIME	签名证书失效时间
ENC_SUBJECT	数字信封证书主题
ENC_SER_NUMBER	数字信封证书序列号
ENC_ISSUER_SUBJECT	数字信封证书颁发者
ENC_START_TIME	数字信封证书生效时间
ENC_END_TIME	数字信封证书失效时间

B.2.3.2 拆解带格式的原文得到文件

接口名称: `public static Map getFileItemsBytes(byte[] byteResults)`
 功能简介: 拆解带格式的原文,得到原文中的文件项
 参数说明: `byteResults` 原文内容
 返回值: `MAP`; `byte[]`类型的文件名和 `byte[]`类型的文件内容组成的键值对容器
 异常: 不能正常解析原文的情况下抛出 `NetSignAgentException`

B.2.3.3 拆解原文得到表单项

接口名称: `public static byte[][] getFormItemsBytes(byte[] byteResults)`
 功能简介: 拆解带格式的原文,得到原文中的表单项
 参数说明: `byteResults` 原文内容
 返回值: `Byte[][]`;表单项(字节流)
 异常: 不能正常解析原文的情况下抛出 `NetSignAgentException`

B.2.3.4 从结果中得到 byte 类型的数据

接口名称: `public byte[] getByteArrayResult(String key)`
 功能简介: 得到响应中的数据项
 参数说明: `String` 数据项名称(见常量定义)
 返回值: `Byte[]`; `Key` 值所对应的数据(字节流)
 异常: 该项数据不是字节流格式或者无此数据项

B.2.3.5 从结果中得到字符串类型的数据

接口名称: `public String getStringResult(String key)`
 功能简介: 得到响应中的数据项
 参数说明: `String` 数据项名称(见常量定义)

返回值: String:Key 值所对应的数据(字符串)
 异常: 该项数据不是字符串格式或者无此数据项

B.2.3.6 从结果中获得 X509Certificate 类型的签名证书

接口名称: public X509Certificate getSignCert()
 功能简介: 得到响应中的签名证书
 参数说明: 无
 返回值: X509Certificate:签名证书
 异常: 找不到响应中的签名证书

B.2.3.7 从结果中获得签名证书扩展项的值

接口名称: public String getCertExtensionValue(String OIDValue)
 功能简介: 得到响应中的签名证书中的扩展项
 参数说明: String OIDValue:扩展 OID 值
 返回值: String 扩展值
 异常: 没有该扩展项或扩展项类型不匹配

B.2.4 NetSignAgentException 类

获取错误代码

接口名称: public int getErrorCode()
 功能简介: 获取错误代码
 参数说明: 无
 返回值: int 类型的错误代码

B.2.5 ServerProcessException 类

获取错误代码

接口名称: public int getErrorCode()
 功能简介: 获取错误代码
 参数说明: 无
 返回值: int 类型的错误代码

B.2.6 错误代码

B.2.6.1 NetSignAgentException 错误代码

错误码	错误描述
-1000	非法的 Server IP 地址
-1001	创建 Socket 连接错误
-1002	获取 Socket 连接错误
-1003	发送报文错误
-1004	接收报文错误
-1005	报文对象的类型不存在
-1010	Base64 编码错误
-1011	Base64 解码错误
-1012	压缩错误
1013	解压错误
1014	报文的格式不正确
-1015	加密报文错误
-1016	解密报文错误
-1017	获取证书扩展错误

- 1018 获取响应结果中的 String 类型的数据时出错
- 1019 获取相应结果中的 byte 数组类型的数据时出错
- 1020 解析带格式的验签名,获取表单内容时出错
- 1021 解析带格式的验签名,获取文件内容时出错
- 1022 输入的密文为空

B.2.6.2 ServerProcessException 错误代码

- | 错误码 | 错误内容 |
|---------|-------------------------|
| —100000 | 接收报文时发生的错误,定义的数据类型不存在 |
| —100001 | 认证客户端错误 |
| —100002 | 系统没有对应的处理器或处理器名称错误 |
| —100004 | 未知错误 |
| —100100 | 错误的输入参数 |
| —100101 | 签名错误 |
| —100102 | 加密证书不匹配 |
| —100103 | 拆解 p7 包出错 |
| —100104 | 签名不正确 |
| —100105 | 证书不被信任 |
| —100106 | 证书已过期 |
| —100107 | 验证 OCSP 出错 |
| —100108 | 证书被作废 |
| —100109 | 解密对称密钥失败 |
| —100110 | 解密数据失败 |
| —100111 | 没有 INFOSEC Provider 提供者 |
| —100112 | 没有对应的算法 |
| —100113 | 私钥不正确 |
| —100114 | 签名错误 |
| —100115 | 加密 Key 出错 |
| —100116 | 加密数据出错 |
| —100117 | 生成数据包出错 |
| —100200 | Server 不能加密数字信封 |
| —100201 | Server 不能进行签名 |
| —100202 | Server 不能解密数字信封 |
| —100203 | 无法找到加密数字信封的公钥证书 |
| —100204 | 无法找到签名用的私钥 |
| —100205 | 没有传递证书(验裸签) |
| —100206 | 系统不支持的数据通信模式(系统不支持加密传输) |
| —100207 | 不合法的数据通信模式 |
| —100208 | 报文内容为空值 |
| —100209 | 对称密钥为空值 |
| —100210 | 对称密钥的摘要为空值 |
| —100211 | 生成对称密钥错误 |
| —100212 | 解密报文错误 |
| —100213 | 加密报文错误 |

100214	压缩报文错误
100215	解压报文错误
100216	Server 未配置时间戳服务
100217	连接时间戳服务器错误
100218	时间戳服务器内部错误
100219	TSA 内容为空值
100220	验 TSA 失败

B.3 烟草行业证书数字签名服务设备 .Net 接口

B.3.1 概述

数字签名服务 .Net 接口提供如下的类供应用使用：

类名	说明
NetSignAgent	数字签名系统客户端接口主类
NSMessageOpt	数字签名系统客户端结果类
ConnectionParameter	数字签名系统的网络连接参数类
NetSignAgentException	数字签名系统客户端异常
ServerProcessException	数字签名系统服务器端异常

B.3.2 ConnectionParameter 类

获得服务器网络连接参数

接口名称： ConnectionParameter.GetInstance(String ip,int port,int maxConnections)

功能简介： 获取包含网络连接参数的对象

参数说明： port 端口
maxConnections 最大连接数

返回值： ConnectionParameter 类型的连接参数对象

B.3.3 NetSignAgent 类

B.3.3.1 初始化 Agent

接口名称： public static void Initialize(ConnectionParameter cp1)

功能简介： 用网络连接参数初始化 Agent

参数说明： cp—网络参数对象

返回值： 无

异常： 无

B.3.3.2 Attached 方式验签名

接口名称： public static NSMessageOpt AttachedVerify(String signedText,String tsaText, bool needCert)

功能简介： 对输入的签名先作 Base64 解码、验签,同时校验签名证书的签名、有效期、证书链的有效性以及 CRL

参数说明： signedText base64 后的签名数据
tsaText base64 后的时间戳签名,如果输入值为 null 则不验证时间戳
needCert 是否返回用于验证签名的公钥证书

返回值： NSMessageOpt 对象,包含以下内容：
byte[]类型的原文
X509Certificate 类型的用于验证签名的公钥证书

String 类型的时间戳生成时间
 String 类型的证书主题
 String 类型的证书序列号
 String 类型的证书颁发者主题
 String 类型的证书有效期起始时间
 String 类型的证书有效期终止时间
 异常: NetSignAgentException: API 端异常
 ServerPorcessException: Server 端处理异常

B.3.3.3 Detached 方式验签名

接口名称: public static NSMessageOpt DetachedVerify(byte[] plainText, String signedText, String tsaText, bool needCert)
 功能简介: 对输入的签名先做 Base64 解码、验签,同时校验签名证书的签名、有效期、证书链的有效性以及 CRL
 参数说明: plainText—原文
 signedText—base64 后的签名数据
 tsaText—base64 后的时间戳签名,如果输入值为 null 则不验证时间戳
 needCert—是否返回用于验证签名的公钥证书
 返回值: NSMessageOpt 对象,包含以下内容:
 X509Certificate 类型的用于验证签名的公钥证书
 String 类型的时间戳生成时间
 String 类型的证书主题
 String 类型的证书序列号
 String 类型的证书颁发者主题
 String 类型的证书有效期起始时间
 String 类型的证书有效期终止时间
 异常: NetSignAgentException: API 端异常
 ServerPorcessException: Server 端处理异常

B.3.3.4 RAW 方式验签名

接口名称: public static NSMessageOpt RawVerify(byte[] plainText, String signedText, String tsaText, byte[] cert)
 功能简介: 对输入的签名先做 Base64 解码、验签,同时校验签名证书的签名、有效期、证书链的有效性以及 CRL
 参数说明: plainText—原文
 signedText—base64 后的签名数据
 tsaText—base64 后的时间戳签名,如果输入值为 null 则不验证时间戳
 cert—der 编码的证书
 返回值: NSMessageOpt 对象,包含以下内容:
 String 类型的时间戳生成时间
 异常: NetSignAgentException: API 端异常
 ServerPorcessException: Server 端处理异常

B.3.3.5 制作数字信封

接口名称: public static NSMessageOpt MakeEnvelope(byte[] plainText, String subject, String sAlg)

- 功能简介：对输入的原文做数字信封，再做 Base64 编码，返回编码结果
- 参数说明：plainText—原文
subject—用于 RSA 加密的公钥证书的主题
sAlg 用于对成加密的对称算法
- 返回值：NSMessageOpt 对象，包含以下内容：
Base64 后的数字信封
- 异常：NetSignAgentException; API 端异常
ServerPorcessException; Server 端处理异常

B.3.3.6 制作带签名的数字信封

- 接口名称：public static NSMessageOpt MakeMSEnvelope(byte[] plainText, String signSubject, String encSubject, String digestAlg, String sAlg)
- 功能简介：对输入的原文做 attached 方式签名的数字信封，再将该数字信封作 Base64 编码并返回编码结果
- 参数说明：plainText—原文
signSubject 用于签名的私钥对应的公钥证书的主题
encSubject 用于 RSA 加密的公钥证书的主题
digestAlg—摘要算法
sAlg 用于对成加密的对称算法
- 返回值：NSMessageOpt 对象，包含以下内容：
Base64 后的数字信封
- 异常：NetSignAgentException; API 端异常
ServerPorcessException; Server 端处理异常

B.3.3.7 解数字信封

- 接口名称：public static NSMessageOpt DecryptEnvelope(String encText, String subject)
- 功能简介：解数字信封
- 参数说明：encText—数字信封
subject—用于解密数字信封的私钥对应的公钥证书的主题
- 返回值：NSMessageOpt 对象，包含以下内容：
byte[]类型的原文
String 类型的证书主题
String 类型的证书序列号
String 类型的证书颁发者主题
String 类型的证书有效期起始时间
String 类型的证书有效期终止时间
- 异常：NetSignAgentException; API 端异常
ServerPorcessException; Server 端处理异常

B.3.3.8 解带签名的数字信封并验签名

- 接口名称：public static NSMessageOpt DecryptMSEnvelope(String encText, String subject)
- 功能简介：对输入的带签名的数字信封先做 Base64 解码，然后解密并验证该数字信封，同时校验签名证书的签名、有效期、证书链的有效性以及 CRL
- 参数说明：encText—数字信封
subject—用于解密数字信封的私钥对应的公钥证书的主题
- 返回值：NSMessageOpt 对象，包含以下内容：

byte[]类型的原文
 String 类型的签名证书主题
 String 类型的签名证书序列
 String 类型的签名证书颁发者主题
 String 类型的签名证书有效期起始时间
 String 类型的签名证书有效期终止时间
 String 类型的加密证书主题
 String 类型的加密证书序列号
 String 类型的加密证书颁发者主题
 String 类型的加密证书有效期起始时间
 String 类型的加密证书有效期终止时间
 异常: NetSignAgentException: API 端异常
 ServerPorcessException: Server 端处理异常

B.3.3.9 Attached 签名

接口名称: public static NSMessageOpt AttachedSignature(byte[] plainText, String subject, String digestAlg, bool uSetSA)
 功能简介: 对输入的原文做 attached 方式签名, 再将签名的结果做 Base64 编码, 并返回编码结果
 参数说明: plainText—原文
 subject—签名证书主题
 digestAlg—摘要算法
 uSetTSA—是否请求 TSA 服务
 返回值: NSMessageOpt 对象, 包含以下内容:
 String 类型的 Base64 后的签名结果
 String 类型的 Base64 后的时间戳
 异常: NetSignAgentException: API 端异常
 ServerPorcessException: Server 端处理异常

B.3.3.10 Dateched 签名

接口名称: public static NSMessageOpt DetachedSignature(byte[] plainText, String subject, String digestAlg, bool uSetSA)
 功能简介: 对输入的原文做 detached 方式签名, 再将签名的结果做 Base64 编码, 并返回编码结果
 参数说明: plainText—原文
 subject—签名证书主题
 digestAlg—摘要算法, 为 null 时使用 SHA1
 uSetTSA—是否请求 TSA 服务
 返回值: NSMessageOpt 对象, 包含以下内容:
 String 类型的 Base64 后的签名结果
 String 类型的 Base64 后的时间戳
 异常: NetSignAgentException: API 端异常
 ServerPorcessException: Server 端处理异常

B.3.3.11 RAW 签名

接口名称: public static NSMessageOpt RawSignature(byte[] plainText, String subject, bool uSetSA)

- 功能简介: 对输入的原文做 RAW 方式签名,再将签名的结果做 Base64 编码,并返回编码结果
- 参数说明: plainText—原文
subject—签名证书主题
uSetTSA 是否请求 TSA 服务
- 返回值: NSMessageOpt 对象,包含以下内容:
String 类型的 Base64 后的签名结果
String 类型的 Base64 后的时间戳
- 异常: NetSignAgentException:API 端异常
ServerPorcessException:Server 端处理异常

B.3.3.12 获得版本号

- 接口名称: public static String GetVersion()
- 功能简介: 获取版本号
- 参数说明: 无
- 返回值: String 类型的版本号
- 异常: 无

B.3.3.13 拆解原文获得文件

- 接口名称: public static Hashtable GetFileItemsBytes(byte[] byteResults)
- 功能简介: 拆解带格式的原文,并且返回所有文件的内容
- 参数说明: byteResults—原文
- 返回值: Hashtable;byte[]类型的文件名和 byte[]类型的文件内容组成的键值对容器
- 异常: 无

B.3.3.14 拆解原文获得表单项

- 接口名称: public static byte[][] GetFormItemsBytes(byte[] byteResults)
- 功能简介: 拆解带格式的原文,得到原文中的表单项
- 参数说明: byteResults 原文内容
- 返回值: Byte[][]:表单项(字节流)
- 异常: 不能正常解析原文的情况下抛出 NetSignAgentException

B.3.4 NSMessageOpt 类

B.3.4.1 获取原文数据

- 接口名称: public byte[] GetPlainText()
- 功能简介: 获取原文数据
- 参数说明: 无
- 返回值: byte[]类型的原文
- 异常: 无

B.3.4.2 获得 TSA 结果

- 接口名称: public byte[] GetTSAText()
- 功能简介: 获取 TSA 结果
- 参数说明: 无
- 返回值: Byte[]类型的 TSA 结果
- 异常: 无

B.3.4.3 获取 DER 编码的签名证书

- 接口名称: public byte[] GetCert()
- 功能简介: 获取 DER 编码的签名证书

参数说明： 无
返回值： Byte[]类型的签名证书
异常： 无

B.3.4.4 获取 X509 格式的签名证书

接口名称： public X509Certificate GetX509Cert()
功能简介： 获取签名证书的 X509 对象
参数说明： 无
返回值： X509Certificate 类型的签名证书对象
异常： 无

B.3.4.5 获得加密证书的主题

接口名称： public String GetEncSubject()
功能简介： 获取加密证书主题
参数说明： 无
返回值： String 类型的加密证书主题
异常： 无

B.3.4.6 获取签名证书的主题

接口名称： public String GetSignSubject()
功能简介： 获取签名证书的主题
参数说明： 无
返回值： String 类型的签名证书的主题
异常： 无

B.3.4.7 获取生成 TSA 的时间

接口名称： public String GetTSAGenerateTime()
功能简介： 获取生成 TSA 的时间
参数说明： 无
返回值： String 类型的生成时间
异常： 无

B.3.4.8 获取签名证书的序号

接口名称： public String GetSignSerNumber()
功能简介： 获取签名证书序号
参数说明： 无
返回值： String 类型的签名证书序号
异常： 无

B.3.4.9 获取签名证书颁发者的证书主题

接口名称： public String GetSignIssuerSubject()
功能简介： 获取签名证书颁发者的证书主题
参数说明： 无
返回值： String 类型的签名证书颁发者的证书主题
异常： 无

B.3.4.10 获取签名证书有效期的起始时间

接口名称： public String GetSignStartTime()
功能简介： 获取签名证书有效期起始时间
参数说明： 无

返回值: String 类型的起始时间

异常: 无

B.3.4.11 获得签名证书有效期截止时间

接口名称: public String GetSignEndtime()

功能简介: 获取签名证书有效期截止时间

参数说明: 无

返回值: String 类型的截止日期

异常: 无

B.3.4.12 获得加密证书序列号

接口名称: public String GetEncSerNumber()

功能简介: 获取加密证书序列号

参数说明: 无

返回值: String 类型的加密证书序列号

异常: 无

B.3.4.13 获得加密证书的颁发者的主题

接口名称: public String GetEncIssuerSubject()

功能简介: 获取加密证书颁发者主题

参数说明: 无

返回值: String 类型的加密证书颁发者主题

异常: 无

B.3.4.14 获得加密证书有效期开始时间

接口名称: public String GetEncStartTime()

功能简介: 获取加密证书有效期开始时间

参数说明: 无

返回值: String 类型的加密证书有效期开始时间

异常: 无

B.3.4.15 获得加密证书有效期截止时间

接口名称: public String GetEncEndtime()

功能简介: 获取加密证书有效期截止时间

参数说明: 无

返回值: String 类型的加密证书有效期截止时间

异常: 无

B.3.5 NetSignAgentException 类

获取错误代码

接口名称: public int GetErrorCode()

功能简介: 获取错误代码

参数说明: 无

返回值: Int 类型的错误代码

B.3.6 ServerProcessException 类

获取错误代码

接口名称: public int GetErrorCode()

功能简介: 获取错误代码

参数说明: 无

返回值: Int 类型的错误代码

B.3.7 错误代码

B.3.7.1 NetSignAgentException 错误代码

错误码	错误描述
--1000	非法的 Server IP 地址
--1001	创建 Socket 连接错误
--1002	获取 Socket 连接错误
--1003	发送报文错误
--1004	接收报文错误
--1005	报文对象的类型不存在
--1010	Base64 编码错误
--1011	Base64 解码错误
--1012	压缩错误
--1013	解压错误
--1014	报文的格式不正确
--1015	加密报文错误
--1016	解密报文错误
--1017	获取证书扩展错误
--1018	获取响应结果中的 String 类型的数据时出错
--1019	获取相应结果中的 byte 数组类型的数据时出错
--1020	解析带格式的验签名,获取表单内容时出错
--1021	解析带格式的验签名,获取文件内容时出错
--1022	输入的密文为空

B.3.7.2 ServerProcessException 错误代码

错误码	错误内容
--100000	接收报文时发生的错误,定义的数据类型不存在
--100001	认证客户端错误
--100002	系统没有对应的处理器或处理器名称错误
--100004	未知错误
--100100	错误的输入参数
--100101	签名错误
--100102	加密证书不匹配
--100103	拆解 p7 包出错
--100104	签名不正确
--100105	证书不被信任
--100106	证书已过期
--100107	验证 OCSP 出错
--100108	证书被作废
--100109	解密对称密钥失败
--100110	解密数据失败
--100111	没有 INFOSEC Provider 提供者
--100112	没有对应的算法
--100113	私钥不正确

-100114	签名错误
-100115	加密 Key 出错
100116	加密数据出错
100117	生成数据包出错
-100200	Server 不能加密数字信封
100201	Server 不能进行签名
100202	Server 不能解密数字信封
-100203	无法找到加密数字信封的公钥证书
-100204	无法找到签名用的私钥
-100205	没有传递证书(验裸签)
-100206	系统不支持的数据通信模式(系统不支持加密传输)
-100207	不合法的数据通信模式
100208	报文内容为空值
100209	对称密钥为空值
100210	对称密钥的摘要为空值
100211	生成对称密钥错误
-100212	解密报文错误
-100213	加密报文错误
100214	压缩报文错误
-100215	解压报文错误
100216	Server 未配置时间戳服务
100217	连接时间戳服务器错误
-100218	时间戳服务器内部错误
100219	TSA 内容为空值
-100220	验 TSA 失败

B.4 烟草行业安全审计服务 Java 接口

B.4.1 实例化接口(I)

接口名称:	public SnmpTrap(String hostId, String enterprise,int port)
功能简介:	此接口为实例化日志发送类
参数说明:	hostId:安全审计服务的 IP 地址; enterprise:日志发送端的 OID 标识;(1.3.6.1.4.17864.1.4.1.5.1.3) port:安全审计服务的端口(162)
返回值:	无
异常:	无

B.4.2 实例化接口(II)

接口名称:	public void send(String userDn,String userIp,long access_time,String sid,String access_type,String access_result)
功能简介:	此接口是通过 SNMP Trap 方式发送日志
参数说明:	userDn:访问应用系统的用户证书 DN userIp:访问应用系统的用户 IP

access_time: 访问应用系统的时间
sid: 访问的应用系统(1.3.6.1.4.17864.1.4.1.5.1.3)
access_type: 对应用系统的操作类型("login")
access_result: 对应用系统做操作的结果, 成功返回"sucess", 失败返回"failed"

返回值: 无
异常: 无

中 华 人 民 共 和 国 烟 草
行 业 标 准
烟草行业数字证书应用接口规范
YC/T 327 -2009

*

中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045

网址 www.spc.net.cn

电话:68523946 68517548

中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销

*

开本 880×1230 1/16 印张 2.5 字数 65 千字
2010年4月第一版 2010年4月第一次印刷

*

书号:155066·2-20723 定价 36.00 元

如有印装差错 由本社发行中心调换
版权专有 侵权必究
举报电话:(010)68533533



YC/T 327-2009

www.bzxz.net

免费标准下载网