

中国标准化协会标准

CAS

STANDARDS OF CHINA ASSOCIATION
FOR STANDARDIZATION

156-2007

标准电子签名系统应用规范

第 1 部分：IE 应用接口

Standard of Application Specification for
Electronic Signature System
Part 1: IE Application Interface

2007-06-22 发布



索引号

CAS 156-2007 (C)

该标准版权为中国标准化协会所有。除了用于国家法律或事先得到
中国标准化协会文字上的许可外，不许以任何形式再复制该标准。
中国标准化协会地址：北京市海淀区增光路 33 号中国标协写字楼
邮政编码：100037 电话：68481778 68486206 传真：68485356
网址：www.china-cas.org 电子信箱：cas@china-cas.org

前 言

中国标准化协会(CAS)是组织开展国内、国际标准化活动的全国性社会团体。制定中国标准化协会标准(以下简称:中国标协标准),满足企业需要,推动企业标准化工作,这也是中国标准化协会的工作内容之一。中国境内的团体和个人,均可提出制、修订中国标协标准的建议并参与有关工作。

本标准按《中国标准化协会标准管理办法》进行管理,按 CAS1.1—2001《中国标准化协会标准结构及编写规则》的规定编制。

中国标协标准草案经向社会公开征求意见,并得到参加审定会议的75%以上的专家、成员的投票赞同,方可作为中国标协标准予以发布。

本标准规定了标准电子签名系统的IE应用接口,适合于在IE网页上增加电子签名时应用。

在总标题《标准电子签名系统应用规范》下,由以下几个部分组成:

- 第一部分: IE应用接口;
- 第二部分: Office应用接口;
- 第三部分: 智能卡接口;
- 第四部分: USB钥匙接口;
- 第五部分: 安全PC接口;
- 第六部分: CA证书接口。

本标准的附录是一个应用实例。

本标准由中国标准化协会电子签名标准化推进工作组提出。

本标准由中国标准化协会归口。

使用本协会标准的单位,应按国家有关规定办理企业标准备案,并对技术内容负责。

在本标准实施过程中,如发现需要修改或补充之处,请将意见和有关资料寄给中国标准化协会,以便修订时参考。

引 言

标准电子签名系统采用非对称密码技术。它可用来提供实体鉴别、数据原发鉴别、数据完整性鉴别和抗抵赖服务。

标准电子签名系统的特点是在于引入了图形化签名机制。通过这种机制,使得满足此标准的IE网页设计可以直接应用标准电子签名系统的签名卡,进而增加网页签名的便利性。

标准电子签名系统应用规范

第1部分：IE应用接口

1 范围

本部分规定了标准电子签名系统的IE接口，适合于在IE网页上增加电子签名时应用。

本部分不涉及任何具体的密码运算，所有密码运算均在符合国家有关法规的密码设备中进行。

本部分凡涉及密码相关内容，按国家有关法规实施。

2 引用标准

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 15851 信息技术 安全技术 带消息恢复的数字签名方案

GB/T 15843.1 信息技术 安全技术 实体鉴别 第1部分：概述

GB/T 15843.2 信息技术 安全技术 实体鉴别 第2部分：采用对称加密算法的机制

GB/T 15843.3 信息技术 安全技术 实体鉴别 第3部分：用非对称签名技术的机制

GB/T 15843.4 信息技术 安全技术 实体鉴别 第4部分：采用密码校验函数的机制

GB/T 15843.5 信息技术 安全技术 实体鉴别 第5部分：使用零知识技术的机制

GB/T 17901.1 信息技术 安全技术 密钥管理 第1部分：框架

GB/T 17902.1 信息技术 安全技术 带附录的数字签名第1部分：概述

GB/T 17902.2 信息技术 安全技术 带附录的数字签名 第2部分：基于身份的机制

GB/T 17902.3 信息技术 安全技术 带附录的数字签名 第3部分：基于证书的机制

3 术语和定义、缩略语

下列术语、定义和缩略语适用于本文件。

3.1 术语和定义

数据电文 electronic records

以电子、光学、磁或者类似手段生成、发送、接收或者储存的信息。

电子签名 electronic signatures

数据电文中以电子形式所含、所附用于识别签名人身份并表明签名人认可其中内容的数据。

电子签名人 electronic signer

持有电子签名制作数据并以本人身份或者以其所代表的人的名义实施电子签名的人。

公开密钥基础设施 (PKI) public key infrastructure

支持公钥管理体制的基础设施, 提供鉴别、机密性、完整性和不可否认性等安全服务。

认证中心 (CA) certification authority

受用户信任, 负责创建和分配证书的权威机构。

数字证书 (或证书) digital certificate

由国家认可的, 具有权威性、可信性和公正性的第三方证书认证机构 (CA) 进行数字签名的一个可信的数字化文件。数字证书包含有公开密钥拥有者的信息、公开密钥、签名算法和CA的数字签名。

证书验证 certificate validation

确认证书在给定时间有效的过程, 可能包含一个证书认证路径的构造和处理, 确保该路径上的所有证书在给定时间有效 (即证书没有被撤销或者过期)。

证书撤销列表 (黑名单) certificate revocation list (CRL)

一个已标识的列表, 它指定了一系列证书发布者认为无效的证书。

公开密钥 (公钥) public key

用户密钥对中公布给公众的密钥。

私有密钥 (私钥) private key

3.2 在公钥密码体制中, 用户密钥对中仅为该用户所知的密钥。

3.3 缩略语

下列缩略语适用于本文件:

API	应用程序接口 (Application Programming Interface), 简称应用接口
CA	证书认证机构 (Certification Authority)
B/S	浏览器/服务器 (Browser/Server)
C/S	客户端/服务器 (Client/Server)
PKI	公钥基础设施 (Public Key Infrastructure)

4 标准电子签名系统 IE 应用接口

4.1 标准电子签名系统 IE 应用接口体系结构

标准电子签名系统IE应用接口体系结构, 如图所示:

浏览器端

标准电子签名系统IE应用接口的浏览器端以COM控件的方式封装PKI技术,解决网页内容的签字盖章、完整性校验问题,使用环境为Microsoft Internet Explorer 6.0以上。

浏览器端实现的功能包括(但不限于如下功能):

- a) 文档签章: 对需提交的信息进行电子签章,此过程需要签名人的智能卡。
- b) 签章验证: 电子签章的验证。
- c) 查看证书: 任何人都可以查看签名人的数字证书信息;

服务器端

在服务器端提供服务器端验证组件。用户在浏览器端对需向服务器提交的网页内容进行电子签章,并把已签网页提交给服务器,服务器端通过验证电子签章来检查网页内容是否已篡改。

服务器端实现的功能包括:

- a) 电子签章验证: 对电子签章的验证,以判断网页信息是否已篡改。
- b) 签名人数字证书的有效性验证: 判别签名人所使用数字证书是否合法有效。

5 标准电子签名系统 IE 应用接口函数定义

以下所定义的函数,除明确说明外,其接口参数都不能为空。

5.1 浏览器端

浏览器端IE应用接口函数包括以下具体函数:

- 签名函数: CSS_SignData
- Form 签名函数: CSS_SignForm
- 域签名函数: CSS_SignFormFields
- HTML 文档签名函数: CSS_SignInTags
- HTML 文档签名扩展函数: CSS_SignInTagsEx
- 验证函数: CSS_VerifyData
- Form 验证函数: CSS_VerifyForm
- 域验证函数: CSS_VerifyFormFields
- HTML 文档验证函数: CSS_VerifyInTags
- HTML 文档验证扩展函数: CSS_VerifyInTagsEx
- 获取签名图像标识函数: CSS_GetImageIdentity
- 获取签名图像值函数: CSS_GetImageData
- 设置签名图像值函数: CSS_SetImageData
- 获取控件属性值函数: CSS_GetEncodedData
- 设置控件属性值函数: CSS_SetEncodedData
- 设置证书验证地址函数: CSS_SetCertificateURL
- 错误消息函数: CSS_GetErrorMsg()

签名函数: CSS_SignData

函数名称	BOOL CSS_SignData (LPCTSTR strData)
功能简介	对传入明文数据进行数字签名。
参数说明	strData: [in] 待签名的明文数据。
返回值	TRUE: 签名成功。 FALSE: 签名失败。

Form 签名函数: CSS_SignForm

函数名称	BOOL CSS_SignForm (LPCTSTR FormName, LPCTSTR ExcludeName, BOOL bIncHidden)
功能简介	对指定 form 中所有指定输入域内容进行数字签名。
参数说明	FormName: [in] 待签名的 form 的名字。 ExcludeName:[in] 不被签名的字段域列表。如: FirstName, LastName”表示“FirstName”和“LastName”不在被 签名之列。 bIncHidden: [in] True 表示被签名内容含有 Hidden 域; False 表示被签名内容不含有 Hidden 域。
返回值	TRUE: 签名成功。 FALSE: 签名失败。

域签名函数: CSS_SignFormFields

函数名称	BOOL CSS_SignFormFields(LPCTSTR FormName, LPCTSTR IncludeName)
功能简介	对指定 form 中的指定输入域内容进行数字签名。
参数说明	FormName: [in] 待签名的 form 的名字。 IncludeName:[in] 被签名的字段域列表。如:FirstName, LastName” 表示“FirstName”和“LastName”在被签名之列, 其余字段域不 在被签名之列。
返回值	TRUE: 签名成功。 FALSE: 签名失败。

HTML 文档签名函数: CSS_SignInTags

函数名称	BOOL SignInTags(LPCTSTR strBeginTag, LPCTSTR strEndTag)
功能简介	将起始标志和结束标志之间的 Html 文档提取出来, 并进行签章操作。函数只提取第一次出现的起始标志和结束标志之间的 Html 文档。
参数说明	strBeginTag :[in] 起始标志。 strEndTag :[in] 结束标志。
返回值	TRUE: 签名成功。 FALSE: 签名失败。

HTML 文档签名扩展函数: CSS_SignInTagsEx

函数名称	BOOL SignInTagsEx(LPCTSTR strBeginTag, LPCTSTR strEndTag)
功能简介	将起始标志和结束标志之间的 Html 文档提取出来, 并进行签章操作。函数提取第一次出现的起始标志和最后一次结束的标志之间的 Html 文档。
参数说明	strBeginTag :[in] 起始标志。 strEndTag :[in] 结束标志。
返回值	TRUE: 签名成功。 FALSE: 签名失败。

验证函数: CSS_VerifyData

函数名称	BOOL CSS_VerifyData(LPCTSTR strData)
功能简介	对传入数据与控件内部签名值进行验证。
参数说明	strData: [in] 待验证的明文数据。
返回值	TRUE: 验证签名成功。 FALSE: 验证签名失败。

Form 验证函数: CSS_VerifyForm

函数名称	BOOL CSS_VerifyForm(LPCTSTR FormName, LPCTSTR ExcludeName, BOOL bIncHidden)
功能简介	用指定 form 中所有指定输入域内容作为明文数据与控件内部签名值进行验证。待验证 form 中所有域的名字和 Tab 顺序和签名时的 form 必须保持一致。
参数说明	FormName: [in] 待验证的 form 的名字。 ExcludeName:[in] 不被验证的字段域列表。如 FirstName, LastName 表示“FirstName”和“LastName”不在 被验证之列。 bIncHidden: [in] True 表示被验证内容含有 Hidden 域; False 表示被验证内容不含有 Hidden 域。
返回值	TRUE: 验证签名成功。 FALSE: 验证签名失败。

域验证函数: CSS_VerifyFormFields

函数名称	BOOL CSS_VerifyFormFields(LPCTSTR FormName, LPCTSTR IncludeName)
功能简介	用指定 form 中的指定输入域内容作为明文数据与控件内部签名值进行验证。待验证 form 中指定域的名字和 Tab 顺序和签名时的 form 的指定域必须保持一致。
参数说明	FormName: [in] 待验证的 form 的名字。 IncludeName:[in] 被验证的字段域列表。如: FirstName, LastName 表示“FirstName”和“LastName”在被验证之列, 其余字段域不在被验证之列。
返回值	TRUE: 验证签名成功。 FALSE: 验证签名失败。

HTML 文档验证函数: CSS_VerifyInTags

函数名称	BOOL VerifyInTags(LPCTSTR strBeginTag, LPCTSTR strEndTag)
功能简介	将起始标志和结束标志之间的 Html 文档提取出来, 并进行验证。函数只提取第一次出现的起始标志和结束标志之间的 Html 文档。
参数说明	strBeginTag: [in] 起始标志。 strEndTag: [in] 结束标志。
返回值	TRUE: 验证成功; FALSE: 验证失败。

HTML 文档验证扩展函数: CSS_VerifyInTagsEx

函数名称	BOOL VerifyInTagsEx(LPCTSTR strBeginTag, LPCTSTR strEndTag)
功能简介	将起始标志和结束标志之间的 Html 文档提取出来, 并进行验证。函数提取第一次出现的起始标志和最后一次结束的标志之间的 Html 文档。
参数说明	strBeginTag: [in] 起始标志。 strEndTag: [in] 结束标志。
返回值	TRUE: 验证成功; FALSE: 验证失败。

获取签名图像标识函数: CSS_GetImageIdentity

函数名称	BSTR CSS_GetImageIdentity()
功能简介	取得签名图像的唯一标识值。
参数说明	无
返回值	空: 没有签名图像唯一标识值, 此时没有签名。 不空: 签名图像唯一标识值。

获取签名图像值函数: CSS_GetImageData

函数名称	BSTR CSS_GetImageData()
功能简介	取得签名图像的值。
参数说明	无
返回值	空: 没有签名图像识值, 此时没有签名。 不空: 签名图像值。

设置签名图像值函数: CSS_SetImageData

函数名称	BOOL CSS_SetImageData(LPCTSTR strData)
功能简介	设置签名图像值。此方法必须在成功调用 SetEncodedData() 方法后才能调用。
参数说明	strData: [in] 签名图像值。
返回值	TRUE: 设置成功。 FALSE: 设置失败。

获取控件属性值函数: CSS_GetEncodedData

函数名称	BSTR CSS_GetEncodedData()
功能简介	取得除签名图像外其它控件需要的属性值。
参数说明	无
返回值	空: 此时没有签名。 不空: 签名图像值。

设置控件属性值函数: CSS_SetEncodedData

函数名称	BOOL CSS_SetEncodedData(LPCTSTR strData)
功能简介	设置除签名图像外其它控件需要的属性值。
参数说明	strData: [in] 除签名图像外其它控件需要的属性值。
返回值	TRUE: 设置成功。 FALSE: 设置失败。

设置证书验证地址函数: CSS_SetCertificateURL

函数名称	BOOL SetCertificateURL(LPCTSTR strURL)
功能简介	设置签章认证时根证书的 URL 地址。
参数说明	strURL: [in] 根证书的 URL 地址和证书文件名。
返回值	TRUE: 设置成功。 FALSE: 设置失败。

错误消息函数: CSS_GetErrorMsg()

函数名称	BSTR CSS_GetErrorMsg()
功能简介	取得错误代码消息。
参数说明	无。
返回值	空: 此时没有错误消息。 不空: 错误消息。

5.2 服务器端

服务器端以COM控件的方式存在, 提供以下的方法和属性:

属性:

- BSTR PlainMessage: 所签的明文消息
- BSTR ImageIdentity: 签名图像唯一标识值
- BSTR ImageData: 签名图像的值
- BSTR EncodedData: 带有证书的编码数据
- BSTR LastError: 错误描述
- VARIANT_BOOL IsSignatureValid: 签名是否正确有效
- VARIANT_BOOL IsIssuerCertValid: 证书颁发者证书是否有效
- VARIANT_BOOL IsCertChainValid: 证书链是否有效
- VARIANT_BOOL IsCertValid: 签名证书是否有效
- VARIANT_BOOL IsCertTimeValid: 签名证书是否正确有效

方法:

- 获取明文方法: CSS_GetPlainMessage
- 获取签名图像标识方法: CSS_GetImageIdentity
- 获取签名图像值方法: CSS_GetImageData
- 获取编码数据方法: CSS_GetEncodedData
- 验证方法: CSS_VerifyData
- 证书验证方法: CSS_CertVerifySubjectCert
- CRL 验证方法: CSS_CertVerifyCRLRevocation
- 证书有效期验证方法: CSS_CertVerifyTimeValidity

获取明文方法: CSS_GetPlainTextMessage

方法名称	BOOL CSS_GetPlainTextMessage (BSTR bstrOrigMessage, BSTR bstrFieldNameList)
功能简介	从传入的原始消息中取得明文消息值。
参数说明	bstrOrigMessage: [in] 接收到的客户端提交的消息。 bstrFieldNameList: [in] 接收到的客户端提交的消息中需要过滤掉的域的名称列表, 名称之间使用 “,” 间隔。
返回值	TRUE: 成功; FALSE: 失败。

获取签名图像标识方法: CSS_GetImageIdentity

方法名称	BOOL CSS_GetImageIdentity (BSTR bstrImageIdentityName)
功能简介	取得签名图像的唯一标识值。
参数说明	bstrImageIdentityName: [in] 签名图像的唯一标识值域的名称。
返回值	TRUE: 成功; FALSE: 失败。

获取签名图像值方法: CSS_GetImageData

方法名称	BOOL CSS_GetImageData (BSTR bstrImageDataName)
功能简介	取得签名图像的值。
参数说明	bstrImageDataName: [in] 存放签名图像的值的域的名称。
返回值	TRUE: 成功; FALSE: 失败。

获取编码数据方法: CSS_GetEncodedData

方法名称	BOOL CSS_GetEncodedData (BSTR bstrEncodedDataName)
功能简介	取得带有证书的编码数据。
参数说明	bstrEncodedDataName: [in] 存放带有证书的编码数据的域的名称。
返回值	TRUE: 成功; FALSE: 失败。

验证方法: CSS_VerifyData

方法名称	BOOL CSS_VerifyData (BSTR bstrPlainData, BSTR bstrEncodeData)
功能简介	判别签名的数据是否被篡改。
参数说明	bstrPlainData: [in] 明文, 通过组件的属性输入; bstrEncodeData: [in] 带有证书的编码数据, 通过组件的属性输入。
返回值	TRUE: 验证成功; FALSE: 验证失败。

证书验证方法: CSS_CertVerifySubjectCert

方法名称	BOOL CSS_CertVerifySubjectCert (BSTR bstrEncodeData, BSTR bstrIssuerCertFileName)
功能简介	通过证书文件验证证书是否由信赖的证书颁发者所颁发。
参数说明	bstrEncodeData: [in] 带有证书的编码数据, 通过组件的属性输入。 bstrIssuerCertFileName: [in] 颁发者的证书文件名。
返回值	TRUE: 颁发者正确; FALSE: 颁发者不正确。

CRL 验证方法: CSS_CertVerifyCRLRevocation

方法名称	BOOL CSS_CertVerifyCRLRevocation (BSTR bstrEncodeData, BSTR bstrCrlFileName)
功能简介	通过 CRL 文件方式验证给定证书是否在 CRL 列表中。
参数说明	bstrEncodeData: [in] 带有证书的编码数据, 通过组件的属性输入。 bstrCrlFileName: [in] CRL 文件名。
返回值	TRUE: 验证成功; FALSE: 验证失败。

证书有效期验证方法: CSS_CertVerifyTimeValidity

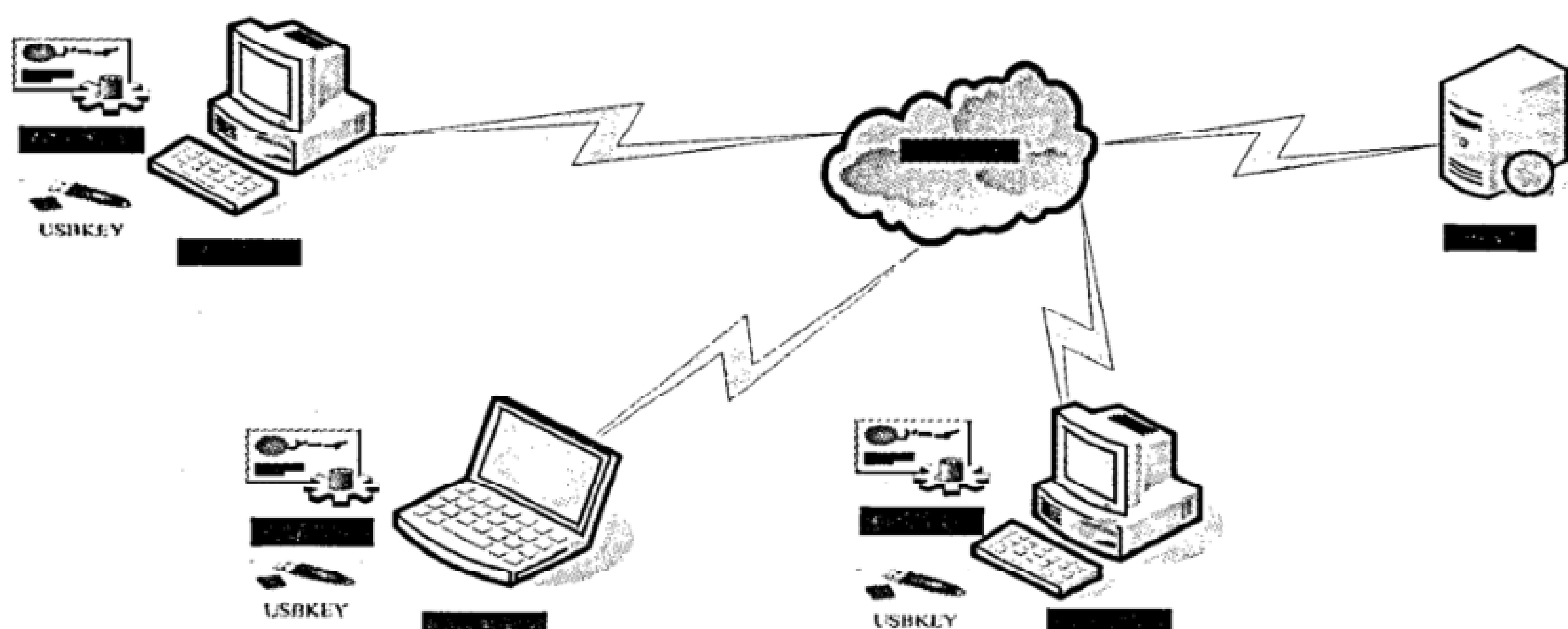
方法名称	BOOL CSS_CertVerifyTimeValidity (BSTR bstrEncodeData)
功能简介	验证给定证书是否在有效期内。
参数说明	bstrEncodeData: [in] 带有证书的编码数据, 通过组件的 EncodedData 属性输入。
返回值	TRUE: 验证成功; FALSE: 验证失败。

附录 A
(资料性附录)

一个应用实例

A.1 ESS网页电子签章系统

ESS网页电子签章系统基于标准电子签名系统IE应用接口实现了对网页内容的电子签章,应用于基于B/S结构的应用系统中。该系统由浏览器端和服务器端两部分组成,用户在浏览器端对需向服务器提交的网页内容进行电子签章,并把已签网页提交给服务器,服务器端通过验证电子签章来检查网页内容是否已篡改。ESS网页电子签章系统的逻辑结构如图所示。



ESS网页电子签章系统是一个可以在网页上对Web页面的表单中的一个或多个域的敏感信息进行数字签名并加盖签名或图章的网页签章系统。

ESS网页电子签章系统在客户端对Web页面的表单中的一个或多个域的敏感信息进行签章操作,然后将产生的签名信息编码后作为请求的一部分传送到服务器端,服务器端对接收到的请求进行验证。在客户端的签章由ActiveX控件完成,在客户端可以对签章进行验证,并支持签章的自动验证。客户端提供了丰富的操作接口,可以对指定输入明文、对指定的输入域及对所有的需要的输入域进行数字签名和内容验证的程序接口。如果选择被签名的原文信息为对所有需要的输入域,则被签名内容包括了http请求部分的主体部分(entity-body),所以不需要程序员指定哪些信息要签名,哪些信息不需要签名。因此,程序员使用本系统时,在客户端的编程将是非常的简单。

而在服务器端,所有的验证工作也由系统自动完成,程序员所要做的只是把验证签名调用简单加在原有程序的前面,不会影响原有的程序的功能。

A.2 ESS网页电子签章系统功能

ESS网页电子签章系统浏览器端提供一个可视化签章控件,主要功能如下:

- a) 能在网页的任意位置上浮透明显示印章或手写签名（简称图章）。具有非常好的视觉效果。未签名前图章可自由移动，签名后图章不能移动；
- b) 文档签章：能对网页 Form 中的指定内容进行数字签名，支持多个单位或个人会签；
- c) 文档验证：能对签署的结果进行完整性认证；
- d) 签章认证：能对图章进行认证，认证图章的真实性、可靠性；
- e) 查看证书：查看签署者个人资料；
- f) 查看签章时间：查看签署者签署文档的时间；

ESS 网页电子签章系统浏览器端操作简单，使用者所有操作通过点击鼠标右键进行，控件界面如下所示，分别为表示签章前和签章后的界面。



ESS 网页电子签章系统服务器端可以对客户端签章的完整性以及签章人证书的正确性进行一系列的验证。

验证工作主要由服务器端的组件完成，通过在网页中添加简单的脚本，即可调用服务器端的组件。具体地，服务器端的组件能够完成如下功能：

- a) 判别签名的数据是否被篡改；
- b) 判别客户端签章用证书颁发者是否正确；
- c) 判别客户端签章用证书是否是信赖 CA 列表颁发；
- d) 判别客户端签章用证书是否在 CRL 列表中；
- e) 判别客户端签章证书是否在有效期内。

CAS 156-2007

本标准起草工作组构成：

主要起草单位： 中国科学院研究生院信息安全国家重点实验室、清华大学、北京诚利通数码技术有限公司

主要起草人： 孙鹏、白国强、陈福林、李津

CAS 156-2007

ICS 35.240

L67

关键词：电子签名、IE 接口、密码运算

STANDARDS OF CHINA ASSOCIATION CAS
FOR STANDARDIZATION 156-2007

Standard of Application Specification for
Electronic Signature System
Part 1: IE Application Interface

First edition
2007-06-22

Reference number
CAS 156-2007(E)



This standard is developed by China Association for Standardization Copyright belongs to China Association for Standardization. All rights reserved. It must not be copied in any form except when it is used in the national laws or used with the permission in word from China Association for Standardization.

China Association for Standardization
No.33 Zengguang Road, CAS Building, Haidian District, Beijing China
Post code:100037
Tel:86-10-68481778 86-10-68486206 Fax:86-10-68485356
Web: www.china-cas.org E-mail: cas@china-cas.org

Foreword

China Association for Standardization (CAS) is a nationwide public organization that organizes and carries out activities about domestic and international standardization. Developing CAS Standard to meet the needs of enterprises and promote the work of enterprise standardization is one of CAS' work contents. Both groups and individuals at home can offer the suggestion on developing or revising CAS standard, and participate in the relevant work.

CAS standard is managed according to "Management Rules for the Standards of CAS", and developed on the basis of CAS 1.1—2001 "Rules for the structure and drafting of standards of CAS".

The draft of CAS Standard is open to the society for suggestion. Only with the vote of more than 75 percent experts and members who attend the Meeting can the draft be issued as the CAS Standard.

This standard specifies the IE interface of electronic signature system.

Under the general title "standard of application specification for electronic signature system", there are several parts as follow:

Part I: IE application interface

Part II: Office application interface

Part II: SmartCard interface

Part IV: USB key interface

Part V: Security PC interface

Part VI: CA certificate interface

The annex of this standard is an application example.

This standard is proposed by Electronic Signature Standardization Promoting Workgroup of China Association for Standardization.

Organizations adopting CAS Standard should apply the registration of standard in accordance with the current national relevant rule and are in charge of the technical content..

In the process of implementing the standard, please mail the opinion and relevant materials to CAS if you find something to be revised or complemented.

Introduction

The Standard of Electronic Signature System uses Asymmetric Crptography technique. It can be used to provide entity authentication, data origin authentication, data integrity authentication and non-repudiation service.

The Standard of Electronic Signature System is characterized by the introduction of a graphical signature mechanism. Through this mechanism, the IE website design that meets this standard can directly uses the signature card and then the convenience of adding a website signature is improved.

Standard of Application Specification for electronic signature system

Part 1: IE Application interface

1 Scope

This part provides the Standard of IE interface for Electronic Signature System, and it is suitable for adding electronic signature to an IE website.

This part does not involve any specific crypto-operation. All crypto-operations are running in cryptographic equipment that is compliant with the relevant state laws and regulations.

Any content that involves cryptography in this part should be implemented according to the relevant state laws and regulations.

2 Reference standard

The following standards contain provisions that, through reference in this text, constitute provisions of this standard. For dated reference, subsequent amendments to, or revisions of, any of these publications do not apply (excluding corrections), and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. For undated references, the latest edition of the normative document referred to applies.

- GB 15851 Information technology, Security technology, Digital signature scheme with message recovery
- GB/T 15843.1 Information technology, Security technology, entity authentication, Part I: Overview
- GB/T 15843.2 Information technology, Security technology, entity authentication, Part II: Mechanism with symmetric encipherment algorithm.
- GB/T 15843.3 Information technology, Security technology, entity authentication, Part III: Mechanism with asymmetric signature technology.
- GB/T 15843.4 Information technology, Security technology, entity authentication, Part IV: Mechanism with cryptographic check function
- GB/T 15843.5 Information technology, Security technology, entity authentication, Part V: Mechanism with Zero-knowledge technology
- GB/T 17901.1 Information technology, Security technology, key management, Part I: Framework
- GB/T 17902.1 Information technology, Security technology, digital signature with appendix, Part I: Introduction
- GB/T 17902.2 Information technology, Security technology, digital signature with appendix, Part II: Mechanism based on identity.

GB/T 17902.3 Information technology, Security technology, digital signature
with appendix, Part II: Mechanism based on certificate

3 Terms and definitions and abbreviations

Following Terminology, definitions and abbreviations are used in this document.

3.1 Terminology and definitions

3.1.1 electronic records

Informations that are generated, sent, received or stored using electronic, optics, magnetism or similar means.

3.1.2 electronic signatures

Data that are included or attached in electronic form in order to identify the signer and show that the signer recognizes data in the content.

3.1.3 electronic signer

The person who has the generative data of electronic signature and implements the electronic signature as himself or as a representative.

3.1.4 public key infrastructure (PKI)

Infrastructures that support public key mechanism and provide authentication, confidentiality, integrity, non-repudiation and other security services.

3.1.5 certification authority (CA)

Authority that is trusted by users and in charge of the generation and allocation of certificates.

3.1.6 digital certificate (or certificate)

A trusted digital document that is digitally signed by a CA which is recognized by the state and has authority, creditability and impartiality. A digital certificate has the information of the public key owner, public key, signature algorithm and the digital signature of CA.

3.1.7 certificate validation

A procedure to confirm the certificate is valid during given period, which could possibly include construction and process of a certification path, in order to ensure that all the certificates in that path are valid during given period (which means the certificate is not revoked or expired).

3.1.8 certificate revocation list (CRL or Black list)

An identified list, which indicates series of certificates that are considered to be invalid by the certificate promulgator.

3.1.9 private key

The key between the key pair that is only known by this user (in public key mechanism).

3.1.10 public key

The key between the key pair that is published to the public(in public key mechanism).

3.2 Abbreviations

The following abbreviations are used in this document.

API	(Application Interface), interface for short
CA	(Certification Authority)
B/S	(Browser/Server)
C/S	(Client/Server)
PKI	(Public Key Infrastructure)

4 The standard of IE application interface for electronic signature system

4.1 The system structure of IE application interface for electronic signature system

The system structure of the standar of Application Specification for electronic signature system is shown in figure 1.

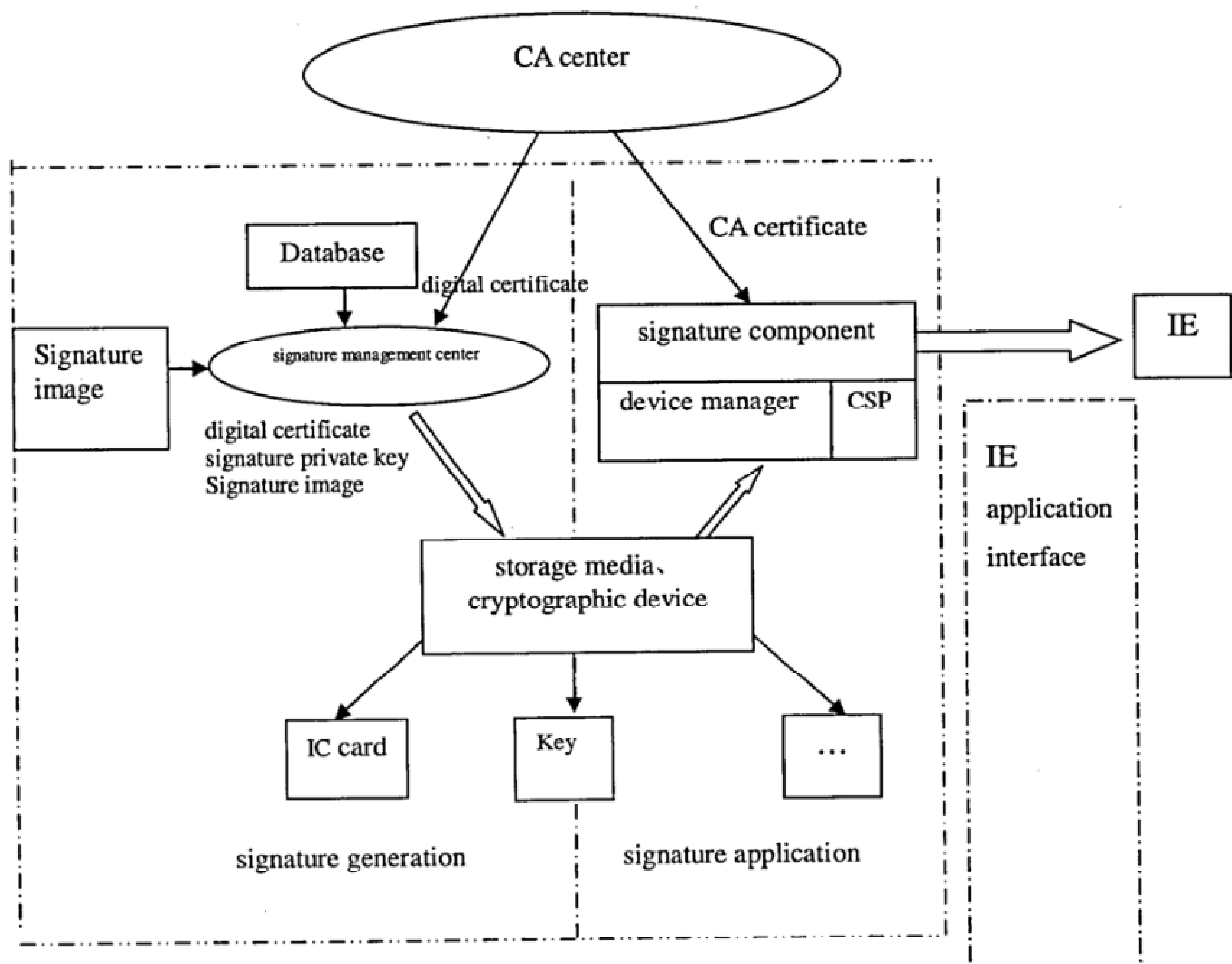


Figure1 The system structure of ofthe standard of IE application interface for electronic signature system

IE application interface of electronic signature system is located between application system and cryptographic device. IE applications implement electronic signature, signature verification and certificate verification by calling IE application interface of IE application interface of electronic signature system. IE application interface of electronic signature system implements specific crypto-operation and key application in cryptographic device through standard interface.

IE application interface of electronic signature system of the standard covers the differences among various devices(encryption machine, encryption card, smart IC card and smart USB key, etc),covers the differences between cryptographic device and cryptographic application interface and realized the irrelevance between application program and cryptographic device by supporting CSP interface style.

IE application interface of electronic signature system of the standard uses digital signature technology. The digital signature should follow the provisions of state standard GB 15851-1995 ,GB/T 15843 and GB/T 17902.

The message functions provided by IE application interface of electronic signature system of the standard follow the format of PKCS#7.

4.2 The components and function explanations of IE application interface of electronic signature system of the standard.

IE application interface of electronic signature system of The standard consists of two parts as follow:

- browser
- server

4.2.1 browser

Browser of IE application interface of electronic signature system of The standard encapsulates the PKI technology in COM control way. It solves the problem of signature and seal and integrity checking of website content. It should be used in Microsoft Internet Exploer 6.0 or later version.

Functions implemeted by Browser include(But not limited to following functions):

- a) Document signature:To implement electronic signature on submitted message, and this procedure needs the smart card of the signer.
- b) Signature verification: the verification of the electronic signature.
- c) View the certificate: Any user can view the digital certificate information of the signer.

4.2.2 server

The server provides server verification component.User implements the electronic signature on the web pages which needs to be submitted to the server and submits the signed pages to the server through browser. Server checks whether the webpages have been illegally modified by verifying the electronic signature.

The functions that server provides include:

- a) Signature verification: Verifying the electronic signature, in order to check if the web page messages have been illegally modified.
- b) Validity verification of the signer's digital certificate: Checking whether the signer's digital certificate is legally valid.

5 Function interface definition of IE application interface of electronic signature system of The standard

The interface parameters of the functions defined in next part can't be void except it is clearly stated.

5.1 Browser

The IE application interface functions in browser include following functions:

- Signature function: CSS_SignData
- Form signature function: CSS_SignForm
- domain signature function: CSS_SignFormFields
- HTML document signature function: CSS_SignInTags
- HTML document signature expansion function: CSS_SignInTagsEx
- verification function: CSS_VerifyData
- Form verification function: CSS_VerifyForm
- domain verification function: CSS_VerifyFormFields
- HTML document verification function: CSS_VerifyInTags
- HTML document verification expansion function: CSS_VerifyInTagsEx
- Get signature image identity function: CSS_GetImageIdentity
- Get signature image data function: CSS_GetImageData
- Set image data function: CSS_SetImageData
- Get control property data function: CSS_GetEncodedData
- Set control property data function: CSS_SetEncodedData
- Set certificate verification address function: CSS_SetCertificateURL
- Error message function: CSS_GetErrorMsg()

5.1.1 Signature function: CSS_SignData

Function name	BOOL CSS_SignData (LPCTSTR strData)
Function introduction	To implements digital signature on imported plain text.
Parameter introduction	strData: [in] The plain text to be signed.
Returned value	TRUE: Signing succeeded FALSE: Signing failed

5.1.2 Form signature function: CSS_SignForm

Function name	BOOL CSS_SignForm (LPCTSTR FormName, LPCTSTR ExcludeName, BOOL bIncHidden)
Function introduction	To implement digital signature on all given input domain content in the given form.
parameter introduction	FormName: [in] The name of the form to be signed. ExcludeName:[in] List of fields and domains that should not be signed. For example, "FirstName,LastName" means "FirstName" and "LastName" should not be signed. bIncHidden: [in] True means the signed content has Hidden domain. False means the signed content does not have Hidden domain.
Returned value	TRUE: Signing succeeded. FALSE: Signing failed.

5.1.3 domain signature function: CSS_SignFormFields

Function name	BOOL CSS_SignFormFields(LPCTSTR FormName, LPCTSTR IncludeName)
Function introduction	To implements digital signature on given input domain in given form.
parameter introduction	FormName: [in] Name of the form to be signed. IncludeName:[in] Signed field list. For example, "FirstName,LastName" means "FirstName" and "LastName" are in Signed list, and the rest field are not.
Returned value	TRUE: Signing succeeded FALSE: Signing failed

5.1.4 HTML document signature function: CSS_SignInTags

Function name	BOOL SignInTags(LPCTSTR strBeginTag, LPCTSTR strEndTag)
Function introduction	Extract the HTML document between the begin tag and end tag, and run the signature operation. This function only extracts the HTML document between the first begin tag and end tag.
parameter introduction	strBeginTag :[in] Begin tag strEndTag :[in] End tag
Returned value	TRUE: Signing succeeded FALSE: Signing failed

5.1.5 HTML document signature expansion function: CSS_SignInTagsEx

Function name	BOOL SignInTagsEx(LPCTSTR strBeginTag, LPCTSTR strEndTag)
Function introduction	Extract the HTML document between the begin tag and end tag, and run the signature operation. This function extracts the HTML document between the first begin tag and the last end tag.
parameter introduction	strBeginTag :[in] Begin tag strEndTag :[in] End tag
Returned value	TRUE: Signing succeeded FALSE: Signing failed

5.1.6 verification function: CSS_VerifyData

Function name	BOOL CSS_VerifyData(LPCTSTR strData)
Function introduction	Verify the imported data and inner signature data of the control.
parameter introduction	strData: [in] Data to be signed
Returned value	TRUE: Signature verification succeeded. FALSE: Signature verification failed.

5.1.7 Form verification function: CSS_VerifyForm

Function name	BOOL CSS_VerifyForm(LPCTSTR FormName, LPCTSTR ExcludeName, BOOL bIncHidden)
Function introduction	Verify the inner signature data of control with the given input domain content in given form as plain text. All the domain name and Tag sequence in the form to be verified must be same as the sequence when it was signed.
parameter introduction	FormName: [in] Name of the form to be verified. ExcludeName:[in] List of the fields that should not be verified. For example ,“FirrstName,LastName” suggest “FirstName”and “LastName”are not to be verified bIncHidden: [in] True suggests the content to be verified has a Hidden domain. False suggests the content to be verified doesn't have a Hidden domain.
Returned value	TRUE: Signature verification succeeded. FALSE: Signature verification failed.

5.1.8 domain verification function: CSS_VerifyFormFields

Function name	BOOL CSS_VerifyFormFields(LPCTSTR FormName, LPCTSTR IncludeName)
Function introduction	Verify the inner signature data of control with the given input domain content in given form as plain text. All the domain name and Tag sequence in the form to be verified must be same as the sequence when it was signed.
parameter introduction	FormName: [in] The name of the form to be verified. IncludeName:[in] The list of the verified field. For example, FirstName and LastName suggests "FirstName" and "LastName" are in the list to be verified, and the rest fields are not in the list to be verified.
Returned value	TRUE: Signature verification succeeded. FALSE: Signature verification failed.

5.1.9 HTML document verification function: CSS_VerifyInTags

Function name	BOOL VerifyInTags(LPCTSTR strBeginTag, LPCTSTR strEndTag)
Function introduction	Extract the HTML document between begin tag and end tag, and verify it. This function only extract the HTML document between the first begin tag and first end tag.
parameter introduction	strBeginTag: [in] Begin tag strEndTag: [in] End tag
Returned value	TRUE: Verification succeeded FALSE: Verification failed

5.1.10 HTML document verification expansion function: CSS_VerifyInTagsEx

Function name	BOOL VerifyInTagsEx(LPCTSTR strBeginTag, LPCTSTR strEndTag)
Function introduction	Extract the HTML document between begin tag and end tag, and verify it. This function only extract the HTML document between the first begin tag and the last end tag.
parameter introduction	strBeginTag: [in] Begin tag strEndTag: [in] End tag
Returned value	TRUE: Verification succeeded FALSE: Verification failed

5.1.11 Get signature image identity function: CSS_GetImageIdentity

Function name	BSTR CSS_GetImageIdentity()
Function introduction	Get the unique identity of the signature image
parameter introduction	N/A
Returned value	Void: There is no unique identity of the signature image, which means there is no signature. Not void: the unique identity of the signature image.

5.1.12 Get signature image data function: CSS_GetImageData

Function name	BSTR CSS_GetImageData()
Function introduction	Get the data of the signature image
parameter introduction	N/A
Returned value	Void: there is no signature image data, which means there is no signature Not void: signature image data.

5.1.13 Set image data function: CSS_SetImageData

Function name	BOOL CSS_SetImageData(LPCTSTR strData)
Function introduction	Set the signature image data. This function must be called after successfully calling the SetEncodeData().
parameter introduction	strData: [in] Signature image data
Returned value	TRUE: Setting succeeded FALSE: Setting failed

5.1.14 Get control property data function: CSS_GetEncodedData

Function name	BSTR CSS_GetEncodedData()
Function introduction	Get the properties data that the control needs other than signature image.
parameter introduction	N/A
Returned value	Void: When there is no signature Not void: Signature image data

5.1.15 Set control property data function: CSS_SetEncodedData

Function name	BOOL CSS_SetEncodedData(LPCTSTR strData)
Function introduction	Set the properties data that the control needs other than signature image.
parameter introduction	strData: [in] The property data that the control needs other than signature image.
Returned value	TRUE: Setting succeeded FALSE: Setting failed

5.1.16 Set certificate verification address function :
CSS_SetCertificateURL

Function name	BOOL SetCertificateURL(LPCTSTR strURL)
Function introduction	Set the URL address of the root certificate when the signature is being verified.
parameter introduction	strURL: [in] The URL address and certificate filename of the root certificate.
Returned value	TRUE: Setting succeeded. FALSE: Setting failed.

5.1.17 Error message function: CSS_GetErrorMsg()

Function name	BSTR CSS_GetErrorMsg()
Function introduction	Get the error code message.
parameter introduction	N/A
Returned value	Void: when there is no error message Not void: the error message

5.2 Server

The server exists as COM control and it provides following methods and properties:

Properties:

- BSTR PlainMessage: The signed plain text
- BSTR ImageIdentity: The unique identity of the signature image
- BSTR ImageData: The signature image data
- BSTR EncodedData: The encoded data with certificate
- BSTR LastError: Error description
- VARIANT_BOOL IsSignatureValid: Whether the signature is valid

- VARIANT_BOOL IsIssuerCertValid: Whether the certificate of the certificate promulgator is valid.
- VARIANT_BOOL IsCertChainValid: Whether the certificate chain is valid
- VARIANT_BOOL IsCertValid: Whether the signature certificate is valid
- VARIANT_BOOL IsCertTimeValid: Whether the signature certificate is correct and valid.

Methods:

- Get plain text method: CSS_GetPlainTextMessage
- Get the signature image identity method: CSS_GetImageIdentity
- Get signature image data method: CSS_GetImageData
- Get encoded data method: CSS_GetEncodedData
- Verify the data method: CSS_VerifyData Verify the data
- Verify the certificate method: CSS_CertVerifySubjectCert Verify the certificate
- Verify the CRL method: CSS_CertVerifyCRLRevocation Verify the CRL
- Verify the time validity of the certificate method:
CSS_CertVerifyTimeValidity

5.2.1 Get plain text method: CSS_GetPlainTextMessage

Method name	BOOL CSS_GetPlainTextMessage (BSTR bstrOrigMessage, BSTR bstrFieldNameList)
Function introduction	Get the plain text message data from the imported origin message.
parameter introduction	bstrOrigMessage: [in] Message submitted from the user. bstrFieldNameList: [in] The list of domain name that should be filtered in the user submitted message. The names are separated with “,”
Returned value	TRUE: Succeeded FALSE: Failed

5.2.2 Get the signature image identity method: CSS_GetImageIdentity

Method name	BOOL CSS_GetImageIdentity (BSTR bstrImageIdentityName)
Function introduction	Get the unique identity of the signature image
parameter introduction	bstrImageIdentityName: [in] The unique identity domain name of the signature image.
Returned value	TRUE: Succeeded FALSE: Failed

5.2.3 Get signature image data method: CSS_GetImageData

Method name	BOOL CSS_GetImageData (BSTR bstrImageDataName)
Function introduction	Get the signature image data
parameter introduction	bstrImageDataName: [in] The name of the domain that contain the signature image data
Returned value	TRUE: Succeeded FALSE: Failed

5.2.4 Get encoded data method: CSS_GetEncodedData

Method name	BOOL CSS_GetEncodedData (BSTR bstrEncodedDataName)
Function introduction	Get the encoded data with certificate
parameter introduction	bstrEncodedDataName: [in] The name of the domain that contain the encoded data with certificate.
Returned value	TRUE: Succeeded FALSE: Failed

5.2.5 Verify the data method: CSS_VerifyData

Method name	BOOL CSS_VerifyData (BSTR bstrPlainData, BSTR bstrEncodeData)
Function introduction	Verify whether the signature data has been illegally modified.
parameter introduction	bstrPlainData: [in] Plain text, input through the control property bstrEncodeData: [in] The encoded data with certificate, input through the component property
Returned value	TRUE: Verification succeeded FALSE: Verification failed

5.2.6 Verify the certificate method: CSS_CertVerifySubjectCert

Method name	BOOL CSS_CertVerifySubjectCert(BSTR bstrEncodeData, BSTR bstrIssuerCertFileName)
Function introduction	Verify whether the certificate is promulgated by trusted promulgator by verifying the certificate file.

parameter introduction	bstrEncodeData: [in] Encoded data with certificate, input through the component property bstrIssuerCertFileName: [in] The certificate file name of promulgator.
Returned value	TRUE: The promulgator is correct FALSE: The promulgator is incorrect

5.2.7 Verify the CRL method: CSS_CertVerifyCRLRevocation

Method name	BOOL CSS_CertVerifyCRLRevocation(BSTR bstrEncodeData, BSTR bstrCrlFileName)
Function introduction	Verify whether the given certificate is in CRL list through CRL file.
parameter introduction	bstrEncodeData: [in] The encoded data with certificate, input through the component property. bstrCrlFileName: [in] CRL file name
Returned value	TRUE: Verification succeeded FALSE: Verification failed

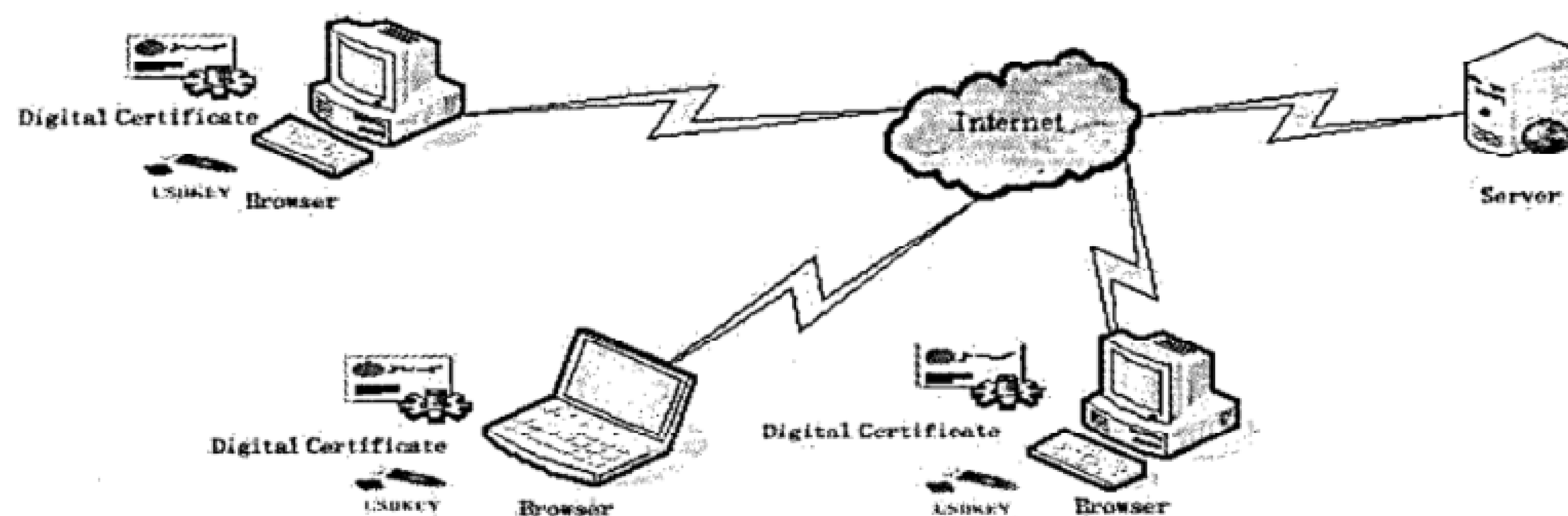
5.2.8 Verify the time validity of the certificate method: CSS_CertVerifyTimeValidity

Method name	BOOL CSS_CertVerifyTimeValidity(BSTR bstrEncodeData)
Function introduction	Verify whether the given certificate is in valid period.
parameter introduction	bstrEncodeData: [in] The encoded data with certificate, input through the EncodedData property of the component.
Returned value	TRUE: Verification succeeded. FALSE: Verification failed.

Annex A
(Informative Annex)
A practical example

A.1 ESS web page electronic signature system

ESS web page electronic signature system is based on electronic signature system of The standard and it implements electronic signature on web pages, and it applies on application system based on B/S structure. This system consists of two parts of server and browser. The user implements electronic signature on web pages needed to be submitted to the server in browser, and submits the signed web pages to server. The server checks whether the web page content has been illegally modified by verifying electronic signature. The logic structure of ESS web page electronic signature system is shown as followed:



ESS web page electronic signature system is a web page signature system that can implement digital signature on sensitive information of one or many domain of Web pages sheet and stamp signature and seal on it.

ESS web page electronic signature system implements signature operation on sensitive information of one or many domain of Web page sheet in client, and then transfer the encoded generated signature information to server as a part of the request. The server-end verifies the received request. The signature operation in client is finished by ActiveX control. Verification could be done in client, and the auto-verification is supported. The client provides various operation interface, and interface that could implement digital signature and content verification on given plain text and given input domain and all needed input domain. If the signed origin text message is chosen as input domain to all needs, the programmer doesn't need to specify which information needs signatures and which information doesn't. Therefore, when programmer uses this system, the operation on client is very easy.

In server-end, all the verification tasks are automatically finished by system. All the programmer need to do is easily adding the calling of signature verification function in the front of the origin program, which will not influence the origin program function.

A.2 ESS web page electronic signature system function

The browser-end of ESS web page electronic signature system provides a visual signature control, whose main functions are shown as followed:

- a) It can display transparent seal or hand-writing signature(stamp for short) at any location of the web page. It has excellent visual effects. The stamp can move freely before signing, and it cannot after signing.
- b) Document signature: It can implements digital signature on given content of web page Form, and it supports co-signing of multi-units and multi-persons.
- c) Document verification: It can verify the integrity of the signing result.
- d) Signature authentication: authenticate the signature, and authenticate the authenticity and the reliability of the signature.
- e) View certificate: View the signer's personal information.
- f) View signing time: View the time when signer signed the document.

The operation on browser-end of ESS web page electronic signature system is easy. All operation of the user could be completed by right-clicking. The control interface is shown as follow, which are the interface before the signing and after the signing respectively.



The server-end of ESS web page electronic signature system could implements series of verification on the integrity of the client signature and validity of the signer's certificate.

The verification tasks are mainly completed by server-end components. The server-end component can be called by easily adding scripts in web pages. The server-end component can complete following functions:

- a) Verify whether the signature has been illegally modified.
- b) Verify whether the promulgator of the client signing certificate is valid.
- c) Verify whether the client signing certificate is promulgated by trusted CA list.
- d) Verify whether client signing certificate is in CRL list.
- e) Verify whether client signing certificate is in valid period.

CAS 156-2007

The WG of the standard consisting of:

Leading drafting units: State Key Laboratory of Information Security of Graduate
University of Chinese Academy of Sciences,
Tsinghua University
Beijing ChengLiTong Digital Technology Ltd.

Main drafters: Guoqiang Bai, Peng Sun, Fulin Chen, Jin Li.

CAS 156-2007

ICS 35.240

L67

Keywords: electronic signature, IE interface, crypto-operations

www.bzxz.net

免费标准下载网