ICS 35.030
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0109—2021

基于云计算的电子签名服务技术要求

Technical requirements for electronic signature service based on cloud computing

2021-10-18 发布　　2022-05-01 实施

国家密码管理局　　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：北京数字认证股份有限公司、数安时代科技股份有限公司、三未信安科技股份有限公司、长春吉大正元信息技术股份有限公司、中金金融认证中心有限公司、中国电力科学研究院有限公司、北京金奥博数码信息技术有限责任公司、杭州天谷信息科技有限公司、浙江汇信科技有限公司、北京国富安电子商务认证有限公司、江苏意源科技有限公司。

本文件主要起草人：李向锋、林雪焰、张永强、傅大鹏、田景成、高志权、赵丽丽、谢吉华、翟峰、王新华、张翼、程亮、王忠义、杨洋、徐冠宁、王胜男。

引　言

近年来，在移动互联网和云计算等新技术的推动下，很多应用领域从业务模式到技术支撑，都发生了深刻的变化，业务越来越需要能够随时、随地开展和确认，而为保障业务合规性和安全性的电子签名技术，也应该及时适应这些变化，在这些新的场景中发挥积极作用。同时，移动互联网业务中，通过电子签名技术保证业务安全性的需求越来越多，电子签名相关应用将向移动互联网延伸。

基于云计算的电子签名，是为业务提供电子签名功能的一种方式。服务方将电子签名以云服务形式提供给用户，使用户能够方便、低成本、随时随地生成各类业务所需的，具有法律效力的电子签名。通过制定本文件，能够对基于云计算的电子签名服务进行规范，从而为业务系统提供便捷可靠的电子签名能力支撑。

基于云计算的电子签名服务技术要求

1 范围

本文件描述了基于云计算的电子签名服务密码技术需求，提出了采用数字证书和数字签名技术实现的基于云计算的电子签名服务的密码技术要求。

本文件适用于指导基于云计算的电子签名服务的建设、管理、检测和应用。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 15843 信息技术 安全技术 实体鉴别

GB/T 20518 信息安全技术 公钥基础设施 数字证书格式

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 25056 信息安全技术 证书认证系统密码及其相关安全技术规范

GB/T 25064 信息安全技术 公钥基础设施 电子签名格式规范

GB/T 31168—2014 信息安全技术 云计算服务安全能力要求

GB/T 32905 信息安全技术 SM3 密码杂凑算法

GB/T 32907 信息安全技术 SM4 分组密码算法

GB/T 32918(所有部分) 信息安全技术 SM2 椭圆曲线公钥密码算法

GB/T 35275 信息安全技术 SM2 密码算法加密签名消息语法规范

GB/T 35276 信息安全技术 SM2 密码算法使用规范

GB/T 36326 信息技术 云计算 云服务运营通用要求

GB/T 37092 信息安全技术 密码模块安全要求

GB/T 38636 信息安全技术 传输层密码协议(TLCP)

GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求

GM/Z 4001 密码术语

3 术语和定义

GM/Z 4001 界定的以及下列术语和定义适用于本文件。

3.1

电子签名 electronic signature

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。

注：本文件中特指采用数字证书和数字签名技术实现的电子签名。

3.2

云计算 cloud computing

通过网络访问可扩展的、灵活的物理或虚拟资源池，并可按需自助获取与管理资源的模式。

注：资源实例包括服务器、操作系统、网络、软件、应用与存储设备等。

3.3

云服务商　cloud service provider

云计算服务的供应方。

注：云服务商管理、运营、支撑云计算的计算基础设施及软件，通过网络支付云计算的资源。

3.4

云服务客户　cloud service customer

为使用云计算服务同云服务商建立业务关系的参与方。

注：本文件中云服务客户简称客户。

3.5

签名方　signer

制作电子签名的实体。

3.6

依赖方　reling party

接受云签名服务的依赖协议，独立地判断电子签名是否满足其应用的安全需求的实体。

3.7

云签名服务　cloud-base signing service

为其他实体提供基于云的电子签名服务及相关服务的机构。

4　缩略语

下列缩略语适用于本文件。

API　应用编程接口(Application Programming Interface)

CA　证书认证机构(Certificate Authority)

CRL　证书吊销列表(Certificate Revocation List)

OCSP　在线证书状态查询协议(Online Certificate Status Protocol)

5　基于云计算的电子签名服务一般架构

5.1　架构模型

基于云计算的电子签名服务是指由云签名服务作为服务方通过云服务方式向客户提供电子签名功能，所提供的电子签名功能称为云签名。在基于云计算的电子签名服务中，各参与方通过交互，完成制作电子签名的操作。

其典型技术框架如图1所示。

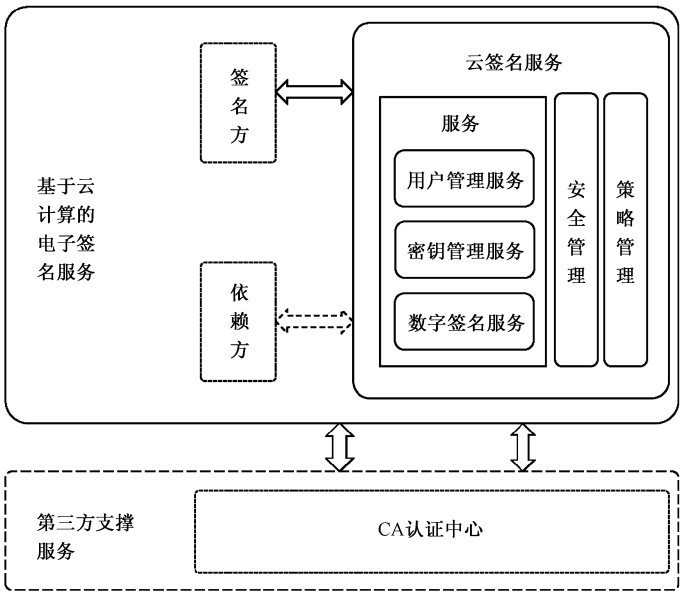

图 1　基于云计算的电子签名服务典型技术框架

基于云计算的电子签名服务典型架构由云签名服务、签名方和依赖方组成，云签名服务提供用户管理服务、密钥管理服务和数字签名服务，并提供与服务相匹配的安全管理和策略管理，签名方和依赖方作为系统的用户，可通过云签名服务的交互协议或应用编程接口（API），使用云签名服务所提供的服务完成电子签名。

图 1 中，CA 认证中心作为第三方支撑服务，用于向签名者提供电子认证服务并对数字证书进行全生命周期管理。

图 1 中，各部分的功能介绍如下：

——签名方在基于云的电子签名活动中，将电子签名功能或电子签名功能的一部分委托云签名服务完成，而签名方使用终端、应用程序或应用系统对制作电子签名的过程进行控制和确认；

——依赖方通过判断签名方或云签名服务提供的电子签名及相关数据有效性来进行后续业务操作；

——云签名服务提供电子签名服务以及相关的用户管理、密钥管理等服务，同时应为云签名服务提供运行支撑。云签名服务以云服务的方式提供，具备云服务按需服务、泛在接入、资源池化、快速伸缩性、服务可计量方面的特性要求。

5.2　服务模式

根据业务场景的不同，云签名服务可以采用不同的模式对外提供服务。常见的服务模式如下。

——协同签名模式：指签名方和云签名服务端各自保存一部分密钥分量，通过密码协议交互产生最终签名结果。详见 A.1。

——代理签名模式：指签名方将密钥托管在云签名服务端，在需要进行电子签名时，授权云签名服务端为其完成签名操作。详见 A.2。

6　依赖方技术要求

依赖方应使用密码模块完成与基于云计算的电子签名过程以及验证签名过程相关的密码功能，密码模块应通过商用密码检测认证，满足 GB/T 37092 中与业务相匹配安全级别的要求。密码模块应支

持依赖方验证电子签名功能，验证电子签名过程应满足 GB/T 25064 的要求。若电子签名功能需要由依赖方发起，密码模块应提供云签名服务接入功能所需的密码功能。

7 签名方技术要求

7.1 总体要求

签名方可使用密码模块完成基于云计算的电子签名所需的密码功能。若使用密码模块，该模块应通过商用密码检测认证，满足 GB/T 37092 中与业务相匹配安全级别的要求，支持 7.2～7.6 的各项要求。

7.2 本地数据保护

签名方应对本地的关键配置数据、敏感数据进行完整性保护和机密性保护。

7.3 身份鉴别

签名方与云签名服务通信时，应支持对云签名服务身份进行鉴别，应按照云签名服务的接入要求声明自身身份。

7.4 通信数据保护

签名方与云签名服务通信时，应按照云签名服务的接入要求进行通信数据保护。

7.5 密钥管理

在使用协同签名模式进行电子签名时，签名方应支持在密码模块内部产生签名密钥的客户端分量，支持密钥分量存储和安全使用。

7.6 电子签名的确认与控制

在电子签名过程中，签名方应对电子签名的相关数据进行确认，并通过交互对签名过程进行控制。若内容确认与签名交互采用密码模块，应满足如下要求：

a) 应支持鉴别所接收到的电子签名请求的来源、确认电子签名报文内容完整性；

b) 在采用协同签名模式时，应保证客户端签名行为与服务端签名行为是匹配的，例如通过对签名的验证确认协同过程是否正常完成。

8 云签名服务技术要求

8.1 概述

云签名服务提供者应建设用于云签名服务的基础设施，设计云签名服务的网络环境和计算环境，实现具备云服务特性的电子签名服务以及相关的用户管理、密钥管理等服务，同时应为云签名服务提供运行支撑。

在云签名服务的建设、运行和服务过程中，应满足 GB/T 22239 中与业务安全要求相匹配的级别要求，满足 GB/T 31168 对云服务安全能力的要求和 GB/T 39786 对密码应用安全的要求。

8.2 建设要求

云签名服务提供者应建设和部署与业务安全级别相匹配的物理环境、基础设施、网络环境和计算环

境，满足 GB/T 39786 对物理环境、网络和通信、设备和计算安全的要求。应通过部署密码模块、密码设备、密码产品或采用第三方密码服务等方式，提供电子签名活动所需的密钥管理、密码运算。所使用的密码模块、密码设备、产品和服务应满足以下要求：

a) 所采用的密码模块应符合 GB/T 37092 与业务安全要求相匹配的级别要求，应通过商用密码检测认证；
b) 所采用的密码设备、密码产品应通过商用密码检测认证；
c) 所采用的商用密码服务应通过商用密码检测认证。

8.3 电子签名服务要求

8.3.1 通用要求

8.3.1.1 密码算法和密码技术的要求

在基于云的电子签名服务中，所采用的密码算法和密码技术、密码协议应符合密码国家标准、行业标准，其中可使用的密码算法包括：

a) 数字签名算法应采用 SM2 椭圆曲线公钥密码算法，符合 GB/T 32918 和 GB/T 35276 的要求；
b) 电子签名过程中数据完整性保护应采用 GB/T 32905 规定的 SM3 密码杂凑算法；
c) 电子签名过程中数据机密性保护应采用 GB/T 32907 规定的 SM4 分组密码算法。

8.3.1.2 电子签名格式要求

云签名服务所形成的电子签名数据应符合 GB/T 25064 或 GB/T 35275 的要求。对于需长期保存的电子签名，电子签名中应包含时间戳和签名时刻的证书状态信息如 CRL、OCSP 响应信息等。

8.3.1.3 数字证书要求

如电子签名需要第三方认证，基于云计算的电子签名服务应采用合法的第三方电子认证机构所颁发的数字证书。云签名服务可与 CA 对接实现用户数字证书的管理。数字证书格式应遵循 GB/T 20518。

8.3.2 用户管理

8.3.2.1 用户注册

云签名服务应支持签名方用户注册到云签名服务中。若存在依赖方发起签名的场景，应支持依赖方用户注册到系统。具体要求如下：

a) 签名方用户注册时，云签名服务应提供签名方用户注册入口，支持用户通过注册入口提交注册信息；
b) 依赖方用户注册时，云签名服务应提供依赖方用户注册入口，支持依赖方提交其注册信息。

8.3.2.2 用户审核

云签名服务应对注册的签名方用户或依赖方用户信息进行审核，确认其是否符合云签名服务的策略要求。

8.3.2.3 用户激活

用户激活时，云签名服务应为签名用户产生用于电子签名的密钥。产生密钥的过程要求详见 8.3.3.2。在协同签名模式下，云签名服务应与签名方进行密钥协商，产生用户签名公钥。用户激活后，

用户可使用此密钥向第三方电子认证机构申请数字证书。

8.3.2.4 用户信息维护

云签名服务应支持用户自主对其自身的信息进行查询、维护和管理。

8.3.2.5 用户注销

云签名服务应支持对用户进行注销。

8.3.3 密钥管理

8.3.3.1 概述

云签名服务应提供满足GB/T 39786中与业务安全级别要求相匹配的签名密钥管理功能，包括密钥产生、密钥存储、密钥使用、密钥备份/恢复、密钥销毁等过程以及运营、运维过程中所需的密钥迁移等，并满足在电子签名过程中密钥由签名者唯一控制的要求。

8.3.3.2 密钥产生

云签名服务为用户产生密钥时，应首先对用户进行基于密码技术的身份鉴别，并通过访问控制确认用户操作是否被允许，确认无误后为用户产生密钥。云签名服务应保证密钥产生过程之间相互隔离，应在日志中记录密钥产生过程，并生成审计信息，审计信息应包括密钥使用的主体、使用的时间等，应保证日志和审计信息不可篡改、不可删除、不可伪造。

对不同签名模式的签名，其密钥产生应满足以下要求。

a) 对协同签名模式，云签名服务应在密码设备中为用户产生服务端密钥分量。在产生密钥的过程中，应保证密钥、密钥分量不以明文形式出现在非专用密码设备的内存或网络中。

b) 对代理签名模式，云签名服务应在密码设备中为用户产生签名密钥。

8.3.3.3 密钥存储

云签名服务应支持存储用户签名密钥或签名密钥的服务端分量，其中私有密钥应加密存储，公开密钥应以数字证书形式存储。应保证用户密钥之间存储隔离。

8.3.3.4 密钥使用

用户签名密钥或签名密钥服务端分量应在用户的授权和控制下使用，仅对用户许可的数据进行签名。具体要求如下。

a) 对于协同签名模式，应使用用户签名密钥的服务端分量进行服务端签名并组合签名结果，可通过云签名服务与签名方分别对待签名数据进行处理保证服务端签名活动只针对特定数据。协议签名过程应保证客户端密钥分量不进行合并，不通过网络传递密钥分量，并保证密钥分量不能通过网络传输的数据计算得到。

b) 对代理签名模式，应在使用密钥前通过密码设备或密码模块进行双因素认证，认证因素与签名者身份、待签名内容、签名时间等信息相关，认证通过后在密码设备或密码模块中完成签名。

c) 应保证密钥的使用过程相互隔离。

d) 应使用密码技术保证在制作电子签名的过程中，签名密钥或签名密钥服务端分量不以明文形式出现在非专用密码设备的内存中或网络上。

e) 应保证云签名服务端不能在用户未授权情况下使用用户密钥来进行签名操作。

f) 应在日志中记录密钥使用情况，并生成审计信息，审计信息应包括密钥使用的主体、使用的时

间等，应保证日志和审计信息不可篡改、不可删除、不可伪造。

8.3.3.5 密钥更新

云签名服务应提供密钥更新服务，密钥更新需要销毁原有密钥并产生新的密钥，申请新的数字证书。密钥的更新应在满足身份认证和访问控制的安全要求下进行。

8.3.3.6 密钥备份与恢复

基于云计算的电子签名服务应制定明确的密钥备份策略，采用安全可靠的密钥备份恢复机制，对密钥进行备份或恢复。其中，系统密钥的备份与恢复应符合 GB/T 25056 的要求。用户签名密钥的密文可采用数据库备份/恢复的方式来进行。密钥备份或恢复应进行记录，并生成审计信息，审计信息应包括备份或恢复的主体、备份或恢复的时间等。

8.3.3.7 密钥销毁

如果用户选择终止云签名服务，应支持销毁用户密钥或用户密钥的服务端分量。密钥销毁应符合 GB/T 25056 的要求。

8.3.4 电子签名过程安全要求

8.3.4.1 概述

在用户产生密钥并获得数字证书之后，云签名服务应支持以云服务方式提供制作电子签名的功能。云签名服务接收签名方或依赖方所发起的电子签名请求，经鉴别和确认无误后，在签名者的确认和控制下进行。电子签名功能应保证用户对签名密钥的唯一控制。

8.3.4.2 签名请求的鉴别

云签名服务在接收到签名请求后，应对请求来源进行鉴别，具体要求如下：

a) 对于依赖方发起的签名，应通过验证数字签名与数字证书确认依赖方身份，验证请求完整性；

b) 对于签名方发起的请求，应识别和验证签名方身份，验证签名请求完整性。

8.3.4.3 电子签名过程要求

电子签名服务过程应使用用户密钥服务端分量或完整的用户密钥进行签名并按约定的格式返回：

a) 对于协同签名模式，应按照 8.3.3.4 中 a)的要求使用用户的签名密钥服务端分量，进行签名，并满足 8.3.3.4 中 c)、d)、e)项的要求；

b) 对于代理签名模式，应按照 8.3.3.4 中 b)的要求使用用户的签名密钥进行数字签名，并满足 8.3.3.4中 c)、d)、e)项的要求。

8.3.4.4 签名过程安全控制

在电子签名过程中，云签名服务应为用户提供各种安全控制措施。

a) 在协同签名模式下，应对协同签名过程进行安全控制，安全控制方法包括但不限于：

   1) 云签名服务对签名方签名行为设置错误计数机制和错误计数上限，当用户签名错误达到错误计数上限则停止为其提供电子签名服务，并提供错误计数清零机制；

   2) 云签名服务应具备识别客户端部分签名结果重放和篡改的能力。

b) 在代理签名模式下，应支持对签名方身份鉴别和签名授权过程进行安全控制，安全控制方法包括但不限于：

1） 云签名服务对签名方身份鉴别和签名授权行为设置错误计数机制，设定错误数上限，当鉴别和授权错误达到错误计数上限则停止为其提供电子签名服务，并提供错误计数清零机制；
2） 云签名服务应具备识别认证和授权数据重放和篡改的能力。

8.3.5 数据安全要求

云签名服务应通过密码技术，对云签名活动涉及的用户数据进行安全保护，应满足 GB/T 39786—2021 的 7.4 中与业务安全要求相匹配级别的要求和 GB/T 31168 的要求，并满足以下要求：

a） 应使用密码技术对个人信息等敏感数据进行脱敏处理；
b） 应支持对数据进行安全隔离，例如采用不同的密钥进行加密；
c） 应对系统的各种日志数据进行完整性保护，保证日志数据不可篡改、不可删除、不可伪造。

8.3.6 电子签名服务接入要求

8.3.6.1 接入身份鉴别

云签名服务接收到服务请求后，应对请求者身份进行鉴别。云签名服务应支持对签名方和依赖方的请求采用不同的身份鉴别机制，身份鉴别可采用 GB/T 15843 规定的机制。

8.3.6.2 接入访问控制

云签名服务应设置访问控制策略，用户的状态和权限，根据不同的请求类型和不同的请求来源，确定如何响应其请求。

8.3.6.3 数据传输要求

云签名服务应采用安全通道与访问者进行通信，例如 GB/T 38636 中定义的传输层密码协议。安全通道应对通信内容进行机密性保护和完整性保护。

8.3.6.4 请求处理与响应

云签名应根据请求类型和不同的请求来源进行相应的处理。请求类型应包括但不限于用户管理、密钥管理和电子签名等，其具体要求见 8.3.2、8.3.3、8.3.4。

8.4 运行支撑要求

8.4.1 安全运营要求

云签名服务提供者应按照 GB/T 36326 要求，对服务相关的人员、流程、资源、技术等要素以及与之相关的场地、网络、数据等方面内容进行规划和管理。包括：

a） 应定义服务能力、服务质量、服务安全能力基线并向相关方公布服务声明；
b） 应确保在签名过程及相关过程中管理员不可使用用户密钥。

8.4.2 安全运维要求

云签名服务提供者应建立安全运维支撑体系，对服务所涉及的各种资源、日志、事件、漏洞以及安全等要素进行维护，以保证云签名服务的服务质量、服务能力和服务安全性。应确保在签名过程中运维人员不可操作用户密钥。

8.5 安全审计要求

云签名服务应提供安全审计功能，对涉及系统安全的行为、人员、时间的日志记录进行跟踪、统计和

分析。安全审计应符合 GB/T 31168—2014 第 11 章的要求，并满足以下要求：

a) 应支持对密钥产生操作、密钥管理操作以及电子签名日志的审计，确认所有密钥操作和电子签名行为是用户发起、控制和确认的，从而保证用户对密钥的控制权；

b) 应支持对云签名服务的运营、管理、维护活动进行审计；

c) 应支持设定云签名服务的审计规则，当触发审计规则时，能够产生报警，云签名服务应将与用户相关的报警信息告知用户。

附 录 A
（资料性）
几种典型的云签名服务模式

A.1 协同签名模式

协同签名模式用于向个人提供签名服务的业务场景。在协同签名模式下，用以电子签名的密钥通常分为服务端分量与客户端分量两个部分，客户端分量存储于用户终端的密码模块中，服务端密钥分量加密存储于云签名服务的密钥库中。在制作电子签名的过程中，在签名方确认下，由客户端和云签名服务共同完成签名。其中客户端使用密码模块进行客户端签名计算，服务端使用密码机完成服务端签名计算，最终合成签名结果。

协同签名模式下，协同密钥管理机制保证了电子签名的密钥不在客户端或服务端出现，密钥的服务端分量、客户端分量不在网络上传输，也不能由网络传输的数据计算得出；协同签名机制保证签名密钥的完整数据不会在客户端和服务端出现，在签名时，客户端和服务端的密钥分量不在网络上传输，也不能由任何传输数据计算得出。

协同签名模式下，签名任务可由依赖方发起或由签名方发起。典型依赖方发起签名请求的协同签名过程如图 A.1 所示。

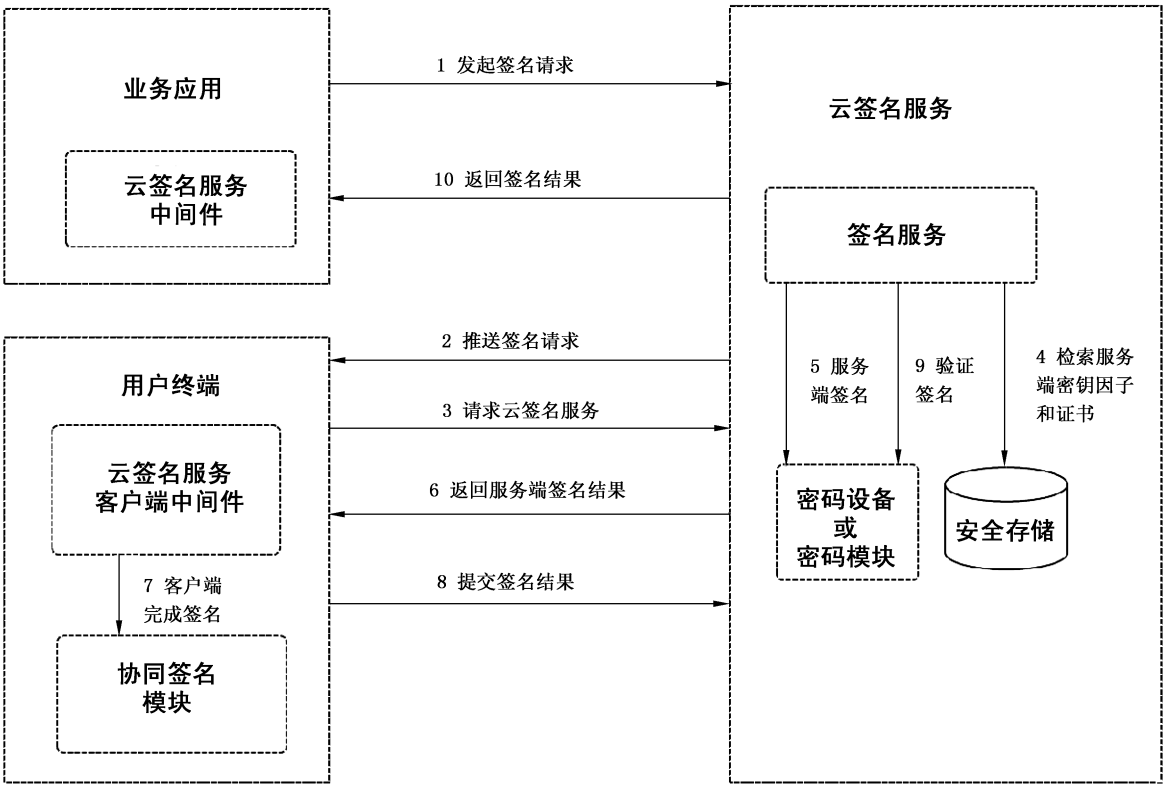

图 A.1 典型协同签名模式示意图

如图 A.1 所示，典型协同签名的过程包括：

a) 业务系统向云签名发起发起签名请求；

b） 云签名服务向签名者终端推送签名请求，此时签名者可通过与签名相关的业务活动情况来对签名请求进行确认；

c） 签名者终端请求云签名服务进行服务端签名；

d） 云签名服务检索该请求者的密钥，得到服务端密钥分量和证书；

e） 云签名服务端进行服务端签名；

f） 云签名服务向签名方返回服务端签名结果；

g） 签名者客户端使用客户端密钥分量完成协同签名；

h） 签名者客户端提交签名结果到云签名服务；

i） 云签名服务验证签名结果，可基于签名验证情况采取安全控制措施；

j） 云签名服务向业务系统返回签名结果。

A.2 代理签名模式

代理签名模式下，用于电子签名的密钥加密保存在云签名服务的密钥库中。在制作电子签名过程中，签名方通过密码技术进行身份确认和授权，在云签名服务完成签名。云签名服务端在密码设备或密码模块中为每个签名操作产生一个动态签名凭据并通过带外通道传递给签名方，凭据与签名者身份、签名数据及时间信息相关联。在签名时，用户向云签名服务提交该凭据以确认签名。

代理签名模式下，签名任务可由依赖方发起或由签名方发起。典型依赖方发起签名请求的代理签名过程如图 A.2 所示。

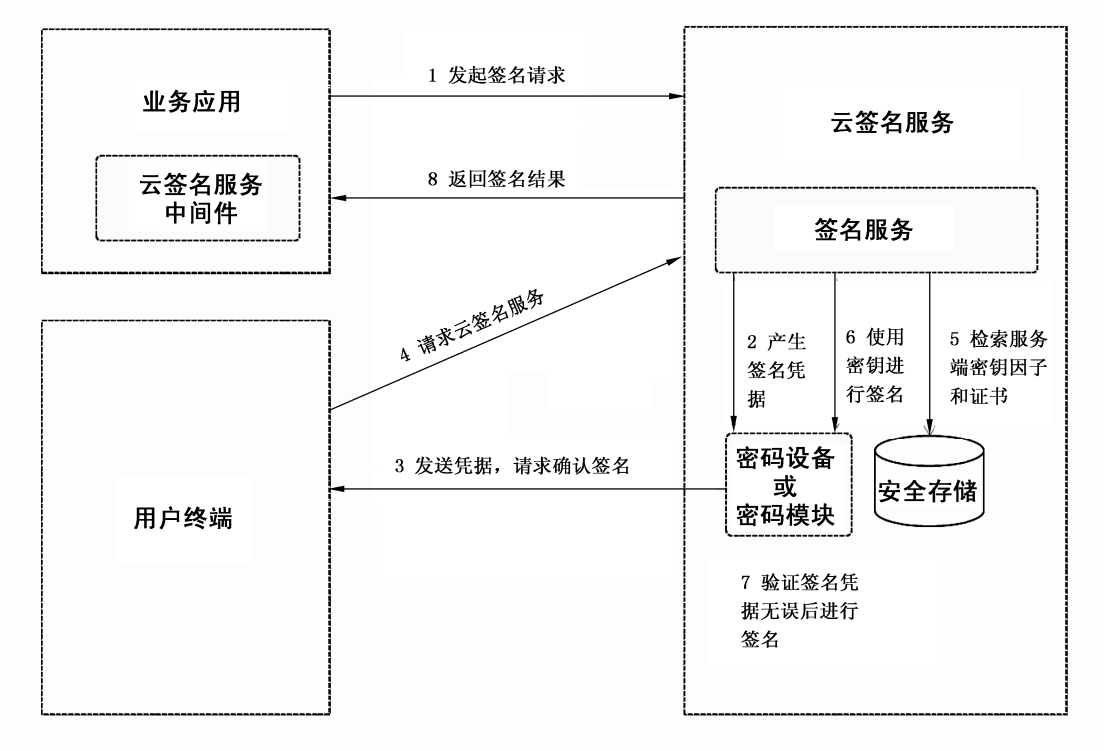

图 A.2 典型代理签名模式示意图

如图 A.2 所示，典型代理签名的过程包括：

a） 业务系统向云签名发起发起签名请求；

b） 云签名服务由密码设备或密码模块为请求者产生一次性签名凭据；

c） 签名者终端向云签名服务请求进行签名；

d) 云签名服务请求密码设备或密码模块进行签名；

e) 云签名服务端的密码设备或密码模块验证签名凭据，若验证无误则进行签名；

f) 云签名服务向业务系统返回服务端签名结果。