ICS 35.030
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0120—2022

基于云计算的电子签名服务技术实施指南

Implementation guidance for electronic signature service based on cloud computing

2022-11-20 发布　　2023-06-01 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。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

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、中国科学院数据与通信保护研究教育中心、北京天融信网络安全技术有限公司、中电科网络安全科技股份有限公司、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、中国电力科学研究院有限公司。

本文件主要起草人：李向锋、林雪焰、张永强、景鸿理、张立廷、傅大鹏、郑昉昱、高志权、赵丽丽、翟峰、刘中。

基于云计算的电子签名服务技术实施指南

1 范围

本文件给出基于云计算的电子签名服务实施可参照的路线和方法。

本文件适用于指导基于云计算的电子签名服务系统的建设和相关产品的开发，对于基于云计算的电子签名服务系统的测试和管理可参照使用。

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 15843.3 信息技术 安全技术 实体鉴别 第3部分：采用数字签名技术的机制

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 20518 信息安全技术 公钥基础设施 数字证书格式

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 25069 信息安全技术 术语

GB/T 25070 信息安全技术 网络安全等级保护安全设计技术要求

GB/T 31168 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 32918.2 信息安全技术 SM2椭圆曲线公钥密码算法 第2部分：数字签名算法

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 信息安全技术 信息系统密码应用基本要求

GM/T 0109—2021 基于云计算的电子签名服务技术要求

GM/Z 4001 密码术语

3 术语和定义

GB/T 25069、GM/T 0109—2021、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。

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，通过网络交付云计算的资源。

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　relying 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-based 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。

3.8

协同签名　collaborate signature mechanism

签名方与云服务各自保存部分密钥分量，通过相互协同配合完成电子签名的机制。

3.9

代理签名　delegated signature mechanism

签名方将密钥托管在云服务，授权云服务完成电子签名的机制。

3.10

原子操作　atomic operation

不可中断的一个或一系列操作。

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）

CPU：中央处理器（Central Processing Unit）

HTTPS：安全超文本传输协议（Secure Hypertext Transfer Protocol）

IMEI：国际移动设备识别码（International Mobile Equipment Identity）

IMSI：国际移动用户识别码（International Mobile Subscriber Identity）

IPSec：IP 安全（IP Security）

JSON：使用 JavaScript 语法描述的数据交换格式（JavaScript Object Notation）

KEK：密钥加密密钥（Key Encryption Key）

OTP：一次性口令（One Time Password）

PIN：个人识别码（Personal Identification Number）

SDK：软件开发工具包（Software Development Kit）

SMK:系统主密钥(System Main Key)
SSL:安全套接层(Secure Socket Layer)
TLCP:传输层密码协议(Transport Layer Cryptography Protocol)
USK:用户签名密钥(User Signing Key)
VPN:虚拟专用网(Virtual Private Network)

5 总则

基于云计算的电子签名服务可根据相关业务系统的网络安全等级保护级别要求以及GM/T 0109的要求,遵循GB/T 39786对相应级别物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全四个层面的要求进行规划和实施。

a) 选择合适的物理场所,遵循GB/T 25070建设与业务安全级别相匹配的基础设施,基础设施包含用于物理和环境安全防护的能力,符合GB/T 39786对物理和环境的要求,同时为电子签名服务活动提供所需的密码支撑能力。如果电子签名服务提供者使用第三方提供的物理和环境,可要求其符合GB/T 39786与业务所要求网络安全级别一致的要求。
b) 通过网络分区、网络防护技术,部署防火墙、入侵检测网络防护、网络隔离等技术或产品,对不同的分区采取与业务安全级别相匹配的安全控制和准入措施,同时采取相应的边界防护等机制,以符合GB/T 39786对网络和通信安全的要求。如果电子签名服务提供者使用第三方提供的网络设施,可要求其符合GB/T 39786与业务所要求网络安全级别一致的要求。
c) 通过安全管理和安全运维支撑满足GB/T 39786对设备和计算安全的要求。如果电子签名服务提供者使用第三方提供的设备与计算环境,可要求其符合GB/T 39786与业务所要求网络安全级别一致的要求。
d) 设计、部署和运行云签名服务,云签名服务与签名方和依赖方相互配合完成基于云的电子签名活动:
    1) 云签名服务通过各种密码模块、密码产品和云计算技术,作为签名方和依赖方之外的独立运营者,提供支持多业务系统、多用户使用的电子签名功能以及配套的密钥管理等功能,服务相关的各个系统符合GB/T 39786应用和数据安全的要求;
    2) 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;
    3) 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。
e) 提供与服务相配套的运营管理、运维支持和安全审计,通过对人员、设备、系统等的安全管理、维护以及对系统各类日志的安全审计,符合GB/T 39786安全管理的要求,具体实施方式见第9章。
f) 向相关方公布其服务质量、服务水平和服务安全性声明,接受国家相关部门的检测认证、监管以及第三方的审计。

6 参考架构

云签名服务总体架构可参考图1。

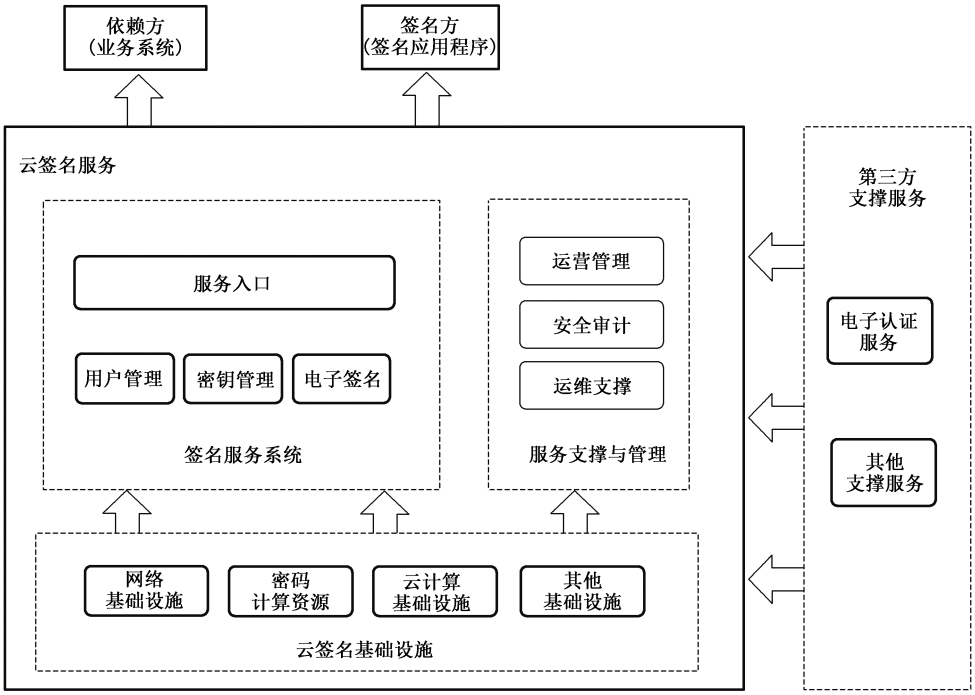

图 1　云签名服务总体架构

在基于云计算的电子签名服务中，云签名服务利用各种基础设施以及第三方的各种支撑，向外提供电子签名功能，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，使用云签名服务所提供的功能进行电子签名。与传统电子签名不同，云签名服务有必要具备同时为多租户服务、密码资源共享、水平扩展等特性。具体实现方式如下：

a) 云签名服务利用云签名基础设施，通过服务系统提供电子签名功能以及相关的用户管理和密钥管理功能，同时提供与服务水平及能力相适应的运营管理、安全审计和运维支撑；

b) 签名方应用程序通过云签名服务提供的编程 API 接口、通信协议或签名模块、签名应用程序，连接到云签名服务完成电子签名功能；

c) 依赖方业务系统通过云签名服务提供的编程 API 接口、通信协议或接入系统，参与电子签名有关的各种过程，完成电子签名功能所需的配合功能；

d) 云签名服务可通过云计算基础设施，采用云架构和云计算技术，使服务具备密码资源共享、水平扩展等特性，支持同时为多租户提供服务，云签名服务可支持 GM/T 0109—2021 中所描述的协同签名模式，或代理签名模式，或其他签名模式；

e) 云签名服务在向外提供服务过程中，可采用第三方的各种服务作为电子签名服务的支撑。例如云签名服务可通过第三方电子认证机构(CA)为云签名服务中的用户以及业务相关方颁发数字证书、提供各种证书服务。

7　云签名基础设施

云签名服务可遵循 GB/T 25070 中所规定的与业务相匹配的级别要求以及业务对服务能力和质量的设计要求，部署网络基础设施、云计算基础设施、密码计算资源以及其他各种基础设施。所部署的基础设施有必要支持水平扩展和弹性服务。

云签名服务在部署密码计算资源时，可采用符合 GM/T 0109—2021 的 8.2 要求的服务器密码机、

签名验签服务器、时间戳服务器、协同签名服务系统、云服务密码机、SSL VPN 等、密码模块或密码系统，以满足电子签名相关的密码需求。可通过由多台密码设备组成密码资源池的方式支持密码能力水平扩展。

8 云签名服务系统

8.1 用户管理

8.1.1 添加用户

云签名服务可支持依赖方业务系统自动添加用户信息，所添加的信息经过依赖方鉴别和核验，云签名服务可支持按照不同的业务系统进行用户分离管理。

8.1.2 用户注册

云签名服务可支持对注册用户进行实名认证和身份核验。用户类型可包括单位用户和自然人用户。用户注册方式可包括授权码注册和自注册两种，可采用如下方式实现。

a) 对于已经在依赖方具有明确身份的签名方，可采用授权码注册的方式完成用户注册。注册授权码由依赖方向云签名服务请求产生，并以带外通道的方式发送给签名方，签名方通过输入注册码来完成云签名服务身份的注册。

b) 对于未在依赖方明确身份的签名方，签名方可在注册时采用云签名服务提供的用户注册功能完成注册和真实身份核验。

c) 对于单位用户，在注册时可指定法定代表人或签名经办人作为签名操作者，或对单位内部相关人员根据需要设置不同的权限级别，云签名服务的注册过程中核验法定代表人及其他人员真实身份、核实经办人单位授权信息。

8.1.3 用户信息管理

云签名服务可支持对用户信息进行管理，可采用如下方式实现：

a) 自然人或单位用户通过操作接口自主对其自身的信息或单位与签名服务相关人员的信息进行查询、维护和管理；

b) 单位用户通过经办人信息管理接口对单位的签名经办人信息进行查询、维护和管理。

8.1.4 用户冻结解冻

云签名服务可通过对用户状态信息按照策略进行变更，以支持对用户进行冻结、解冻。可包括如下情况：

a) 用户自主发起的冻结和解冻；

b) 管理员发起的冻结和解冻。

8.1.5 用户注销

云签名服务可按照策略，标记用户状态为注销状态，同时按照 8.2.2.7 销毁与用户关联的密钥，以支持对用户进行注销。

8.2 密钥管理

8.2.1 密钥体系

8.2.1.1 密钥层次

云签名服务可考虑设计多级密钥管理体系，以实现 GM/T 0109—2021 中 8.3.3 的要求，实现为海

量用户进行电子签名。多级密钥体系可参考本节的方式进行设计。

8.2.1.2 主密钥(SMK)

SMK 是云签名系统的顶级密钥,用以创建和管理密钥加密密钥 KEK。SMK 相关的设计要点包括:

a) SMK 在云签名服务初始化过程中,通过云签名服务的密码机产生;
b) SMK 存储在云签名服务器密码机的非易失性存储中,不支持从密码机导出;
c) 云签名系统可采用备份/恢复方式使所有密码机的 SMK 是相同的;
d) SMK 可根据云签名服务的运营策略和实际情况进行更新,SMK 更新时需要将所有 SMK 加密保护的内容采用新的 SMK 重新进行加密。

8.2.1.3 密钥加密密钥(KEK)

KEK 是云签名系统的中间级密钥,用以加密用户签名密钥或用户签名密钥的服务端分量。KEK 相关的设计要点包括:

a) 第一个 KEK 在云签名服务开始提供服务之前,通过云签名服务密码机产生;
b) 密码机使用主密钥 SMK 加密 KEK 并导出保存在签名服务系统的密钥库中,支持通过运维手段进行密钥的备份/恢复;
c) 云签名系统可支持按照策略分配或更新 KEK 用以加密不同的用户签名密钥或用户签名密钥的服务端分量;
d) KEK 更新后,云签名服务使用新的 KEK 加密存储用户签名密钥或用户签名密钥服务端分量,可保留旧 KEK,对旧 KEK 加密的用户签名密钥或用户签名密钥服务端分量,仍然使用旧的 KEK 解密,也可对加密的用户签名密钥或用户签名密钥服务端分量使用新的 KEK 重新加密存储。

8.2.1.4 用户签名密钥(USK)

USK 是用户签名密钥或用户签名密钥的服务端分量,用以为用户进行电子签名。USK 相关的设计要点包括:

a) 在用户请求产生密钥时,云签名服务在密码机中产生 USK;
b) 对完整的用户签名私钥,可使用密码机的产生密钥功能产生完整的密钥,并标记密钥与用户的关联关系,设置密钥的访问控制策略;对用户签名密钥的服务端分量,可使用协同密钥产生机制在密码机中产生密钥分量,协同签名机制符合 GM/T 0109—2021 第 8.3.3.2 章节 a)的要求,不出现在网络中;
c) 当采用协同签名机制时,云签名服务提供者还需为签名方提供密码模块,用以产生、存储、使用用户签名密钥客户端分量;
d) 密码机采用云签名服务指定的 KEK 加密导出 USK,保存在用户密钥库中,支持通过运维手段进行密钥的备份/恢复;
e) 云签名服务根据用户请求,使用密钥对数据进行签名;
f) 云签名服务根据用户请求或其他管理策略,对 USK 进行生命周期管理。

8.2.2 密钥生命周期管理

8.2.2.1 密钥生成

在用户注册后,云签名服务可在密码模块或密码设备中为用户产生签名密钥或用于协同签名的密

钥分量，具体操作如下：

a) 若产生的密钥为完整的用户密钥，建议在鉴别用户身份后，在用户的授权下为其产生签名密钥，鉴别过程可采用双因素鉴别机制，双因素中一个因素由密码模块或密码设备产生，仅在设定的时间范围内有效，通过带外通道传递给用户；

b) 若产生的密钥为用户协同签名密钥的服务端分量，可采用终端与服务端协同数字签名机制，在密码机中产生服务端分量，在签名方密码模块产生客户端分量。

8.2.2.2 证书申请

云签名服务可为用户提供向电子认证机构申请证书的功能，可在云签名服务集成电子认证机构提供的 SDK，通过 SDK 提供的功能申请证书，需要考虑申请证书过程中电子认证机构与云签名服务之间的身份鉴别、数据安全通信。

8.2.2.3 密钥存储

云签名服务有必要采用密码模块或密码设备中的 KEK 对用户签名密钥或签名密钥的服务端分量进行保护，加密后的密钥数据可保存在密钥库中。可采用如下方式实现：

a) 云签名服务将所产生的签名密钥或协同签名密钥服务端分量加密导出并存储在密钥库中；

b) 云签名服务存储密钥信息、密钥状态，保存该密钥对应的数字证书以保护用户与密钥的关联关系的完整性，建议同时使用数字签名、消息校验码等机制保存其他关联信息的完整性；

c) 签名方采用云签名服务提供者提供的密码模块安全存储用户签名密钥客户端分量，可仅存储部分用以产生用户签名密钥客户端分量的材料，在使用密钥进行协同签名时动态合成；

d) 完整的用户签名公钥，最终以电子认证机构签发的数字证书形式存储，云签名服务、签名方终端、依赖方均可获取。

8.2.2.4 密钥使用

在电子认证机构为用户签发数字证书之后，允许使用该密钥进行电子签名。具体实施方式如下。

a) 在云签名服务需要使用用户密钥进行数字签名时，可通过密钥管理与密码计算解耦的方式，支持密码设备水平扩展，云签名服务从密钥库获得该用户签名密钥或协同密钥的服务端分量的密文，与待签名数据一并送入密码模块或密码设备，完成所需的签名或协同签名过程，密码设备保证密钥的解密和数字签名在隔离的环境中通过原子操作完成。

b) 若使用完整的用户签名密钥进行签名，建议首先由云签名服务系统鉴别用户身份，身份鉴别可通过双因素机制，获得用户的明确授权，在用户参与和控制下解密签名密钥，可考虑双因素中一个因素由密码模块或密码设备产生，与当前时间、待签名内容相关联，通过带外通道传递给用户。密钥使用过程保留从用户鉴别授权到完全签名过程中所有环节的日志，并保障日志不可篡改、不可删除和不可伪造，同时长期保留日志以备审查。

c) 若使用协同签名模式进行签名，可采用终端与服务端协同数字签名机制进行签名操作，在签名过程中，可采用错误计数与设定错误上限策略的方式，拒绝频繁的错误签名请求。

8.2.2.5 密钥更新

当签名方密钥丢失或其他原因不能再使用时，可通过云签名服务支持进行密钥更新。具体更新过程包括：

a) 对用户进行身份鉴别，鉴别通过后为其产生新的签名密钥或协同签名密钥服务端分量；

b) 产生密钥后将新密钥的标识绑定至该用户，同时解除用户与旧密钥的绑定关系；

c) 用户使用新的公钥申请数字证书，可通知电子认证机构同时吊销旧用户证书；

d) 建议同时销毁存储在云签名服务系统中的旧密钥。

8.2.2.6 密钥备份与恢复

云签名服务可采用数据库备份/恢复方法对密钥库进行备份/恢复。

8.2.2.7 密钥销毁

云签名服务可采用多次随机覆盖的方法销毁密钥库中的用户签名密钥或协同密钥服务端分量。

8.3 电子签名

8.3.1 电子签名模式的选择

在基于云计算的电子签名服务体系中，根据签名场景的不同，可采用不同的电子签名模式。可选择的签名模式包括但不限于GM/T 0109—2021所描述的协同签名、代理签名。

8.3.2 协同签名模式

对于为移动终端客户签名的场景，可考虑采用协同签名模式，用户签名密钥由签名者终端和云签名服务各持有一部分分量，由双方协同配合完成签名，其中对端的签名处理中间结果可视为对签名过程的确认信息。附录A中A.1给出了协同签名的应用方案示例，附录B给出了一种典型的协同签名系统设计参考示例，附录C给出了两种典型的协同签名服务的部署示意，具体如下。

a) 签名过程，协同签名典型场景如图2所示。协同签名模式电子签名的过程包括如下内容。

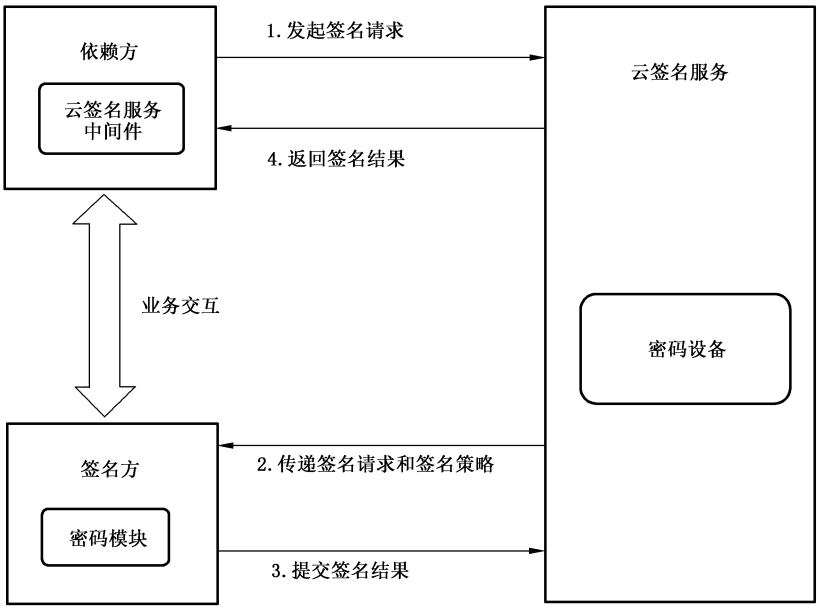

图2 协同签名模式过程示意

1) 当业务需要进行电子签名时，依赖方向云签名服务发起签名请求，请求中可包含签名操作的预期签名者信息，由云签名服务通知签名者进行签名。云签名服务需要对依赖方的身份进行鉴别、验证依赖方签名请求的完整性，确认无误后通知签名者。
2) 签名方接收到依赖方业务过程的签名请求或接收到云签名服务通知的签名任务，在验证签名的业务数据无误后，使用密码模块与云签名服务完成协同签名过程。
3) 云签名服务在签名过程完成后，有必要验证签名正确性以确认签名密钥的客户端分量和服务端分量的匹配关系，仅在验证通过的情况下向签名者或依赖方返回签名结果。

b) 安全性考虑：

1） 协同签名过程可采用终端与服务端协同数字签名的机制，云签名服务采用协同签名服务系统、签名方采用协同签名模块完成签名，协同签名机制符合 GM/T 0109—2021 中 8.3.4.1 对签名必须在用户的确认和控制下进行的要求；
2） 在云签名提供服务的过程中，有必要采取技术手段，防止恶意攻击者修改传输的数据内容，以造成非用户意愿的签名，服务过程可通过身份认证和数据完整性验证以预防此类攻击，同时可支持签名方和依赖方在完成签名后进行验证签名，以确认签名过程无误；
3） 签名过程可同时采用带外通道发送一次性签名凭据例如短信验证码，要求签名者出示该凭据或该凭据的变换形式进行确认；
4） 云签名服务可接收依赖方未经预处理的待签名数据，由云签名服务进行预处理和签名，也可以接收依赖方预处理之后的数据，仅进行签名处理；
5） 云签名服务若在签名后的验签名过程发现错误，及时采取处理措施，如增加错误计数器等，同时向相关方报告错误；
6） 云签名服务设置适当的策略，在发现终端过多错误尝试时可锁定终端或锁定用户，例如终端不断尝试 PIN 码的场景；
7） 云签名服务可通过用户重新鉴别身份支持用户重新产生密钥和重置 PIN 码。

8.3.3 代理签名模式

代理签名模式场景下，签名方将签名密钥托管在云签名服务中，通过远程授权机制进行签名。A.2 给出了代理签名应用方案示例。

a） 签名过程，其典型场景过程示意如图 3 所示。该场景下电子签名过程包括：
1） 当业务需求进行电子签名时，依赖方向云签名服务发起签名请求，请求中包含要求签名者签名的数据；
2） 云签名服务通知签名者进行签名；
3） 签名方接收到签名请求或签名事务通知，验证签名内容，验证无误后，向云签名服务声明身份并授权云签名服务进行电子签名，云签名服务接收到签名方的授权作为对签名过程的确认，完成电子签名；
4） 依赖方从云签名服务获得签名结果，依赖方可使用公钥证书和所发出的签名数据验证电子签名正确性以确认签名过程正确完成。

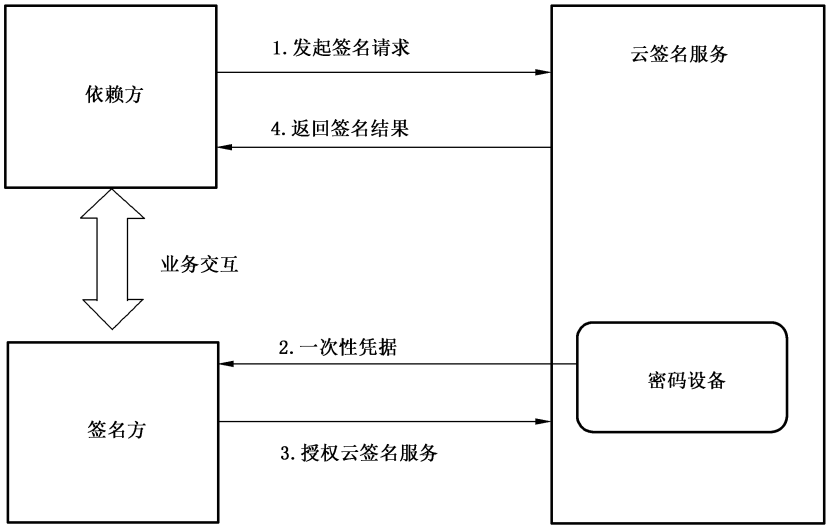

图 3 代理签名模式过程示意

b) 安全性考虑

1) 云签名服务可考虑在签名设备中对签名者进行认证，其鉴别签名者身份的一次性凭据可由签名设备产生，通过带外通道发送给签名者，一次性凭据可采取加密手段防止云签名服务系统其他组件截获、篡改，以保证电子签名符合 GM/T 0109—2021 第 8.3.4.1 的要求；

2) 所发送的一次性签名凭据可与签名者密钥标识、签名内容以及当前时间相关，且具备时效性，支持根据策略限制凭据时间有效期的起始点和终止点，以保证签名授权能够代表签名方身份真实性，授权能够代表签名方对特定数据的签名意愿，电子签名签署过程符合 GM/T 0109—2021 中 8.3.4.1 的要求。

8.4 签名方接入

云签名服务支持签名方在不同的环境中通过网络来使用云签名功能，接入可使用标准的接入方式如通信协议交互、应用编程接口(API)集成或应用程序等，具体如下。

a) 通信协议接入。云签名服务可提供标准的服务接口协议，接收签名方应用程序通过网络向云签名服务发送的签名请求，返回相应的操作结果，协议中支持身份鉴别、数据传输安全保护机制，以符合 GM/T 0109—2021 中 8.3.6 的要求。

b) 应用编程接口集成。云签名服务可提供接口 SDK，支持签名方应用程序在其运行过程中调用接口，完成电子签名所需进行的各种操作，SDK 中包含身份鉴别、数据传输安全保护机制，以符合 GM/T 0109—2021 中 8.3.6 的要求。

c) 应用程序方式。云签名服务可提供接口单独的签名应用程序。签名应用程序提供可视的界面或服务，向操作者或其他应用提供输入接口和功能输出，应用程序支持身份鉴别、数据传输安全保护机制，以符合 GM/T 0109—2021 中 8.3.6 的要求。

8.5 依赖方接入

云签名服务可支持依赖方通过通信协议交互、应用编程接口(API)集成或安全接入前置等方式使用云签名服务向外提供的电子签名相关功能，具体如下。

a) 通信协议接入。云签名服务可提供标准的服务接口协议，接收依赖方向云签名服务发送的请求，返回相应的操作结果。依赖方可采用业务系统环境中部署密码模块或密码产品的方式，以符合 GM/T 0109—2021 中 8.3.6 的要求。

b) 应用编程接口集成。云签名服务可提供接口 SDK，支持签名方应用程序在其运行过程中调用接口，完成电子签名所需进行的各种操作。依赖方可采用业务系统环境中部署密码模块或密码产品的方式，以符合 GM/T 0109—2021 中 8.3.6 的要求。

c) 安全接入前置。云签名服务可提供用于安全接入的前置设备或前置系统，实现依赖方接入云签名服务，云签名服务前置支持接入过程中依赖方用于安全接入云签名服务所需的密钥管理、身份鉴别、安全通信、协议封装等功能，以符合 GM/T 0109—2021 中 8.3.6 的要求。

9 支撑与管理

9.1 运营管理

9.1.1 概述

云签名服务提供者遵循 GB/T 36326 和 GM/T 0109—2021 中 8.4.1 的要求，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。在运营过程中，涉及安全的内容应符合 GB/T 31168 的要求。云签名服务提供者可通过实现安全运营管理系统、建立运

营管理策略的方式，实现所需的各种运营功能。

9.1.2 人员

云签名服务提供者可通过以下机制进行人员管理。

a) 制定人员预算、管理政策与程序。包括建立人员选聘、试用、培训、考核与离职的管理程序，满足业务的人员需求。在需要与第三方合作提供云签名服务的情况下，建立对合作伙伴相关人员的管理制度以对相关人员进行有效管理。

b) 制定人员岗位结构。包括建立专职团队负责云签名服务的提供以及相关技术、管理等事务，对服务过程和相关事务中的不同角色进行明确岗位分工、职责定义，明确对不同岗位的要求。

c) 建立对人员技能的要求与考核机制，保证人员技能能够胜任云签名服务的技术和管理工作要求。

d) 建立人员和岗位的安全管理策略、可信策略，并采取相应的管理控制措施。如对人员可信性，可对正式雇佣的新员工进行可信背景调查，背景调查可分为基本调查和高级调查。可对普通雇员执行基本调查，对关键岗位雇员执行高级背景调查。对关键岗位采用职责分割、双重控制、岗位轮换、最小权限等安全管理措施。

e) 通过制定人员异动管理策略，要求关键岗位设置备份人员，以便在意外情况下使关键业务职能得到延续，避免人员异动发生影响企业运营。

9.1.3 场地管理

云签名服务提供者可通过以下机制进行场地相关的管理。

a) 制定物理场地授权与访问规定，合理控制物理场地权限。

b) 根据内部人员的工作需要，赋予其访问相应物理场地的权限。对没有访问物理场地某区域权限而确因工作需要访问该场地区域的内部人员，在访问该区域时，可由具有相应权限的人员全程陪同，并做好访问记录。

c) 对外来人员出入，可由云签名服务方陪同员工负责填写其进出云签名服务场所的日志。云签名服务通过对所有外来人员进入、离开云签名服务方的场地进行记录，实现对全部访问行为的审计，同时定期将访问控制记录归档、保存以备核查。

9.1.4 网络管理

云签名服务提供者可通过以下机制进行网络管理：

a) 可在网络环境中配置防火墙、入侵防御、漏洞扫描、网页防篡改、安全接入网关和身份认证系统，并从安全区域划分、接入层安全、服务器区的安全和安全管理等多方面加强云签名服务系统的防护；

b) 可采用 VPN 网关，用户通过 VPN 连接到云签名服务系统；

c) 可通过技术手段检测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月。

9.1.5 流程管理

云签名服务提供者可通过如下方式对服务的运营管理层流程进行规划和管理。

a) 云签名服务目录的管理。可通过服务目录的方式，声明或发布云签名服务所提供各种云签名服务以及相关功能的定义、服务能力、服务质量、服务级别，明确服务过程中相关各方的角色与职责。

b) 服务质量、服务能力和服务级别的管理。包括为每个服务定义服务协议、持续监控和报告、定

期或不定期的评估评审等机制。

c) 服务变更需求的管理。包括建立各种服务变更需求的识别、审核、分级、分派，以及从技术和非技术环境对请求进行审批的机制，建立请求的实现流程，规范请求的关闭条件与要求。

d) 服务报告的管理。建立对服务级别的达成情况、服务变更需求满足情况等状态的报告机制，建立服务报告的管理流程，包括建立、审批、分发、归档、评估等，可事先定义报告的内容、范围，定义报告的模板，通过技术手段采集、加工数据形成报告。

e) 服务用户的管理。建立云签名服务用户包括注册、注销和用户信息管理等机制，建立对用户账户的计费、账单查询等机制，建立对服务资源的购买、使用以及退订等机制，建立服务系统的资源监控等机制。

f) 服务计费的管理。可建立根据不同的服务类型设定不同的计费模式和服务计量计费管理机制，包括数据采集、费用计算等，建立账单管理和缴费管理机制。

9.1.6 技术管理

云签名服务提供者可通过如下方式对服务采用的各种技术进行规划和管理：

a) 通过构建网络资源池、存储资源池和计算资源池，实现资源共享，通过密码资源资源池实现密码计算和密钥管理功能的共享和按需分配；

b) 在服务过程和相关过程中，所采用的密码技术均经过国家密码主管部门核准，所采用的密码产品和第三方密码服务均通过检测认证；

c) 通过密码技术确保在业务过程以及相关过程中的数据安全存储与安全管理、安全传输、身份鉴别、访问控制，在涉及用户信息收集的场景中，保证用户隐私信息的安全；

d) 设定不同服务类型的服务计量机制和计量方法、计量指标以对服务进行计量，如资源使用时长、资源使用数量等；

e) 通过对服务进行实时监测，采集、整合服务的性能数据，通过监控数据可对服务性能、服务质量以及故障情况提供分析，可提供可视化或数据级别的对外接口、界面，可采用监测数据存档的方式对服务进行事后分析；

f) 通过对服务系统网络、计算、存储等环节的负载情况进行监控，根据监控数据适时调整网络带宽、计算资源、存储空间，以保证服务水平；

g) 可采用物理隔离、虚拟机隔离、进程隔离等多种机制保证多租户的资源、数据之间的相互隔离。

9.1.7 资源管理

云签名服务提供者可通过如下方式对服务运行所依赖的资源进行规划和管理：

a) 建立对服务环境中网络资源、存储资源和计算资源的计量机制和方法，设定资源使用指标，以支持结合服务能力和质量的要求对服务资源进行容量规划和管理；

b) 建立对服务的运行监控和预警的机制，对资源进行配置调整或进行故障转移处理。

9.2 运维支撑

9.2.1 运维支撑概述

云签名服务提供者有必要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，以符合 GM/T 0109—2021 中 8.4.2 的要求。可通过建设部署安全运维系统实现安全运维的各种功能。可使用数字签名、数字证书以及符合标准要求的密码模块、密码产品保证运维过程中的身份鉴别、通信安全以及不可否认。

9.2.2 资源管理

云签名服务提供者可通过对服务以及相关过程所依赖的各种资产、资源进行识别、分类、分级，明确其所有权、责任者，明确计算资产之间的关联以及资产价值，对于涉及秘密的信息和敏感信息的资产，管理过程中可建立与安全级别相适应的处置规程来进行管理。

9.2.3 日志管理

云签名服务提供者可对服务过程以及相关过程、系统以及设备中产生的日志进行全面收集、归一化预处理，通过具备防篡改、防删除、防伪造的机制存储并按照分析策略进行多维度分析。

9.2.4 身份鉴别与访问控制

云签名服务提供者可通过建立运维角色的身份鉴别机制与对物理环境、设备和云签名服务相关信息系统的访问控制策略，实现对运维角色的身份鉴别和访问控制。

9.2.5 漏洞管理

云签名服务提供者可通过漏洞扫描工具或其他渠道，及时发现与了解系统脆弱性，对系统存在或潜在的漏洞进行评估，并及时加以处置。

9.2.6 备份管理

云签名服务提供者可通过如下机制对服务以及相关活动的资源和数据进行备份管理：

a) 可根据服务水平和服务级别的要求，采用完全备份、差异备份或增量方式对系统进行备份；
b) 可根据服务水平和服务级别的要求，选择同城备份或异地备份；
c) 可根据服务水平和服务级别的要求，建立演练机制。

9.2.7 安全事件管理

云签名服务提供者可考虑采用一致的方式对安全事件进行管理，确保快速、有效和有序地响应安全事件。可通过部署安全事件管理系统、设置安全事件处理策略的方式，实现对安全事件地监视、发现、分析、处理和报告信息安全事态和事件。

9.3 安全审计

云签名服务提供者可通过对业务、运营、管理以及运维日志的审计，保证系统按照规范和既定策略运行，以符合 GM/T 0109—2021 中 8.5 的要求。包括：

a) 通过对密钥产生操作、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都是用户发起、控制和确认的，从而保证用户对密钥的控制权；
b) 通过对系统运行日志和业务日志的日志审计功能，使运维人员能够实时监测系统运行日志，便于快速处理系统的异常。

10 通用技术指南

10.1 密码算法

在基于云计算的电子签名服务中，建议使用国家密码管理部门核准的密码算法完成所需的电子签名以及相关功能，包括如下内容。

a) 采用 SM2 数字签名算法，完成业务所需的数字签名、内部管理操作的身份鉴别。算法遵循

GB/T 32918.2 和 GB/T 35276。

b) 使用 SM3 密码杂凑算法，完成业务所需密码杂凑计算以及数字签名、内部管理操作的身份鉴别以及数据内部存储和传输过程中的完整性保护。算法遵循 GB/T 32907。

c) 使用 SM4 分组密码算法，完成电子签名过程中数据的安全传输、安全存储以及密钥管理。算法遵循 GB/T 32905。

10.2 身份鉴别

基于云计算的电子签名服务中，针对不同的场景对身份鉴别有不同的要求，可采用不同的方式来设计和实现。

a) 可采取基于数字签名的鉴别机制对依赖方进行鉴别，过程可采用 GB/T 15843.3 或 GB/T 15843.4 规定的鉴别机制。依赖方可采用签名验签服务器、服务器密码机等进行身份鉴别所需的密钥管理和密码操作。

b) 针对 8.3 中两种不同的签名模式，可通过如下方式对签名方的身份进行鉴别：

1) 在协同签名模式下，云签名服务在不同的业务过程中可支持不同的鉴别机制，如 OTP 方式、GB/T 15843.4 所规定的机制，或基于协同数字签名算法的方式；

2) 在代理签名模式下，可由云签名服务中的密码设备产生与签名者身份、签名内容、签名时间相关联的一次性凭据，通过带外通道发送给客户，客户在签名时出示该凭据或该凭据的变换形式。

c) 云签名服务内部运营管理、运维支撑、安全审计过程中采用 GB/T 15843.3 规定的鉴别机制。在鉴别过程中，鉴别客户端侧可采用智能密码钥匙等介质进行身份鉴别所需的密钥管理和密码操作。

10.3 安全通信

在基于云计算的电子签名服务、运维、运营和管理活动中，建议采用安全通道进行数据通信和传输，安全通道可遵循 GB/T 38636，或在传输之前对数据源进行加密。具体包括：

a) 云签名服务的管理、运营、运维等活动，可通过部署 SSL VPN 或 IPSec VPN 等产品，实现双向通道；

b) 各类业务应用接入基于云签名服务，可通过在云签名服务侧和业务应用侧分别部署 SSL VPN 或 IPSec VPN 产品的服务端和客户端，实现安全通道；

c) 签名方接入云签名服务，可通过在云签名服务侧部署 SSL VPN 或 IPSec VPN 等产品，签名方部署软件或硬件密码模块，实现单向或双向安全通道；

d) 可通过签名方或依赖方部署的密码模块，采用数字信封等安全机制保护传输的数据。

10.4 密码模块和产品

在基于云计算的电子签名服务、运维、运营和管理活动中，建议采用符合 GB/T 37092 中与业务相匹配的安全级别要求的各类密码模块、密码设备、密码产品，可包括但不限于：

a) 部署于云签名服务系统中的服务器密码机、签名验签服务器、时间戳、云密码机等产品；

b) 用于云签名服务运营管理、运维、审计的智能密码钥匙等；

c) 用于终端客户端与服务器协同签名模块等。

10.5 数字证书

基于云计算的电子签名服务中所使用的用户签名证书可从合法的电子认证机构获得，证书格式遵循 GB/T 20518。云签名服务可将电子认证机构证书服务的接口集成到签名模块或签名应用中，以简

化用户操作流程。

10.6 电子签名格式

建议电子签名格式遵循 GB/T 25064，其中的数字签名遵循 GB/T 35276 和 GB/T 32918.2，数字签名可按照 GB/T 35275 所规定的签名消息语法进行封装。

10.7 云计算特性

10.7.1 密码资源层

可采用如下机制，实现计算资源池化共享、弹性计算以及密码资源按需分配：

a) 部署支持虚拟化的服务器密码机、签名验签服务器等密码设备、密码模块具备虚拟化功能，使之同时为多个请求者进行密钥操作和签名操作，从而实现资源共享；

b) 部署通用的密码机、签名验签服务器等密码设备、密码模块，在密码设备和密码模块之上部署服务层作为云签名密码服务入口，在服务层采用虚拟化、分布式资源管理、微服务等技术实现密码设备计算能力调度。

10.7.2 电子签名服务层

可采用如下机制，为多业务系统、海量用户同时提供密码功能：

a) 借助 10.7.1 所描述的密码资源层，通过逻辑封装实现电子签名服务提供给请求者；

b) 基于多层次的隔离技术架构提升用户数据、用户进程安全性，满足为多业务系统、多用户同时提供签名服务的要求；

c) 采用自动化运维技术实现服务的高效管理；

d) 基于协议转换等机制，支持用户、应用和业务系统通过不同的网络环境接入。

附 录 A
（资料性）
几种典型的云签名应用方案

A.1 协同签名应用方案

在移动终端环境下，可借助协同签名密码模块，使用协同签名方案完成业务所需的电子签名。密钥分为服务端分量和客户端分量两个部分，客户端分量保存在用户终端的密码模块中，服务端分量加密保存在密钥库中，在密码设备中使用。在进行电子签名的过程中，在签名方确认下，由签名方和云签名服务共同完成签名。

云签名服务可通过技术和管理手段，保证签名密钥服务端分量的安全产生、安全存储和安全管理，保证服务端分量在运营管理、运维支撑等环节不会被违规使用。在交互过程中，通过交互协议，保证服务过程的交互安全。协同签名方案架构如图 A.1 所示。

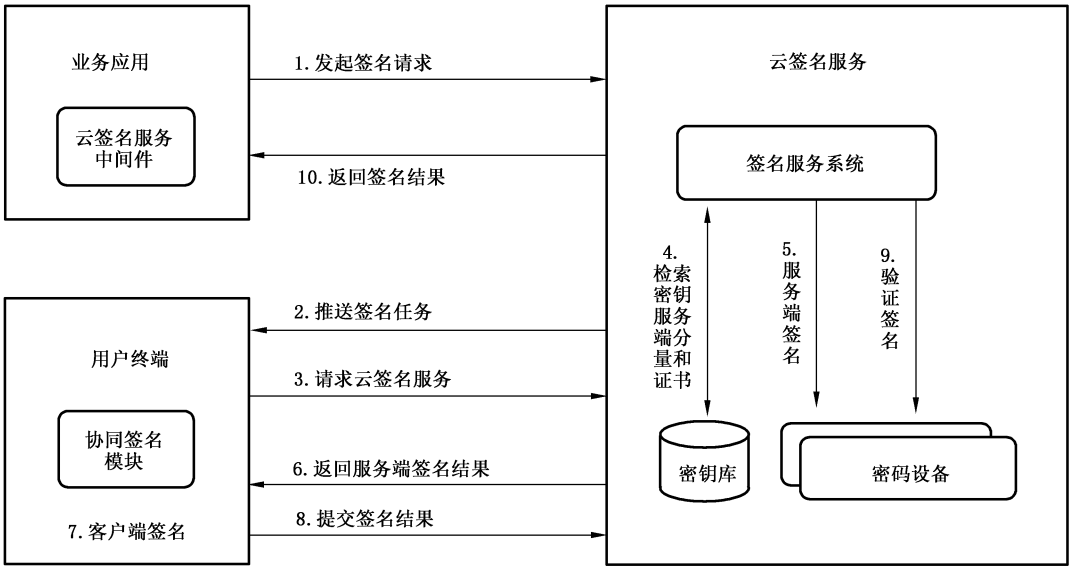

图 A.1 协同签名方案系统架构图

在协同签名方案中，业务系统作为依赖方将电子签名策略、用户信息以及用户证书保存在云签名服务中。用户在移动终端的签名应用中集成云签名的编程接口作为签名方，通过移动终端、云签名服务以及业务系统的配合完成电子签名。具体内容如下。

a) 在业务需要签名时，通过安全通道向云签名服务发送签名请求，请求中指明需要特定或非特定的用户进行签名，云签名服务接收到业务系统的签名请求，验证无误后向业务应用返回签名任务标识。

b) 云签名服务将签名请求提供给签名方。对于特定用户的签名请求，其实现通常的方式包括云签名服务主动推送或签名应用根据业务信息主动获取两种模式，推送信息包括待签名数据、签名策略。对于非特定用户的签名请求，则由业务系统通过业务规则选择用户进行签名。

c) 签名方使用协同签名密码模块，按照签名策略与云签名服务进行协同签名，可按照签名策略封装为业务所需的格式例如 GB/T 35275 的消息语法规范，其过程包括：

1) 签名方请求云签名服务为其进行签名；

2） 云签名服务从密钥库检索用户签名密钥的服务端分量和证书；

3） 云签名服务为使用签名密钥的服务端分量进行协同签名；

4） 云签名服务向签名方返回协同签名中间结果；

5） 签名方本地签名完成最终的签名结果，签名方签名行为可视为签名者对签名的确认；

6） 某些业务可在协同签名机制之外，采用一次性短信口令方式要求签名者对签名进行确认。

d） 签名方提交签名结果到云签名服务。

e） 云签名服务使用该用户的公钥证书，使用密码设备验证签名，验证签名无误可判断签名方和云签名服务的协同正确完成，且签名方持有的密钥分量是正确的。

f） 云签名服务验证无误后将签名结果返回给业务系统。

实际场景中可参照如下方式部署：

a） 云签名服务方可部署 SSL VPN 等产品建立与业务应用、用户终端的安全通道，部署服务器密码机保证用户协同签名密钥服务端分量的安全产生、安全存储、安全使用，保证服务过程和数据存储中的数据完整性以及敏感数据的机密性，部署协同签名服务系统、时间戳产品产生用以完成协同签名和电子签名所需的时间戳；

b） 签名方可采用协同签名密码模块、密码产品协同签名操作；

c） 依赖方可部署 SSL VPN 保证与云签名通信与接入安全，部署签名验签服务器进行电子签名相关操作的数字签名。

A.2 代理签名应用方案

该方案中，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，由云签名服务完成签名。代理签名方案中，提供签名功能的服务方需要保证用户对签名密钥的拥有和控制，保证除密钥的拥有方和合法使用者外，其余实体均不能获取和使用密钥，同时保证签名方的身份鉴别和授权安全，确保签名方的授权不被错误使用。

代理签名方案架构如图 A.2 所示。

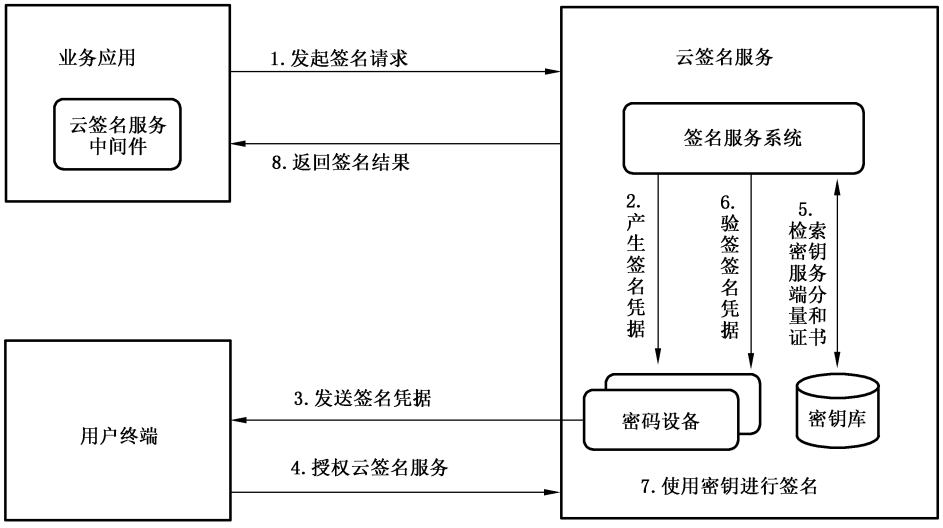

图 A.2 代理签名方案系统架构图

其过程如下：

a） 在业务需要签名时，向云签名发送签名请求；

b） 云签名服务产生与签名者身份、签名数据、签名时间相关联的签名凭据，通过带外通道传递给签名者，例如通过手机发送一次性凭据；

c） 签名者用户终端向云签名服务提交签名请求，请求中包含所收到的签名凭据或凭据的变换形式，作为签名者对签名行为的确认，例如由收到的一次性凭据派生密钥并对数据加密和截取；

d） 云签名服务在签名设备中验证签名凭据，如验证无误则使用该用户的密钥为其签名；

e） 云签名服务向业务返回签名结果。

实际场景中可参照如下方式部署：

a） 云签名服务方可部署 SSL VPN 等产品建立与业务应用、用户终端的安全通道，部署服务器密码机保证用户签名密钥的安全产生、安全存储、安全使用，保证服务过程和数据存储中的数据完整性以及敏感数据的机密性，部署签名验签服务器、时间戳产品产生用以完成电子签名所需的时间戳；

b） 签名方可采用密码模块完成所需的操作；

c） 依赖方可部署 SSL VPN 保证与云签名通信与接入安全，部署签名验签服务器进行电子签名相关操作所需的数字签名。

附 录 B
（资料性）
协同签名方案系统设计参考示例

B.1 概述

在本示例的应用系统中，可以通过手机应用程序与签名服务系统，实现基于移动终端的重要业务抗抵赖及数据完整性保护。

B.2 系统架构

系统架构如图 B.1 所示。

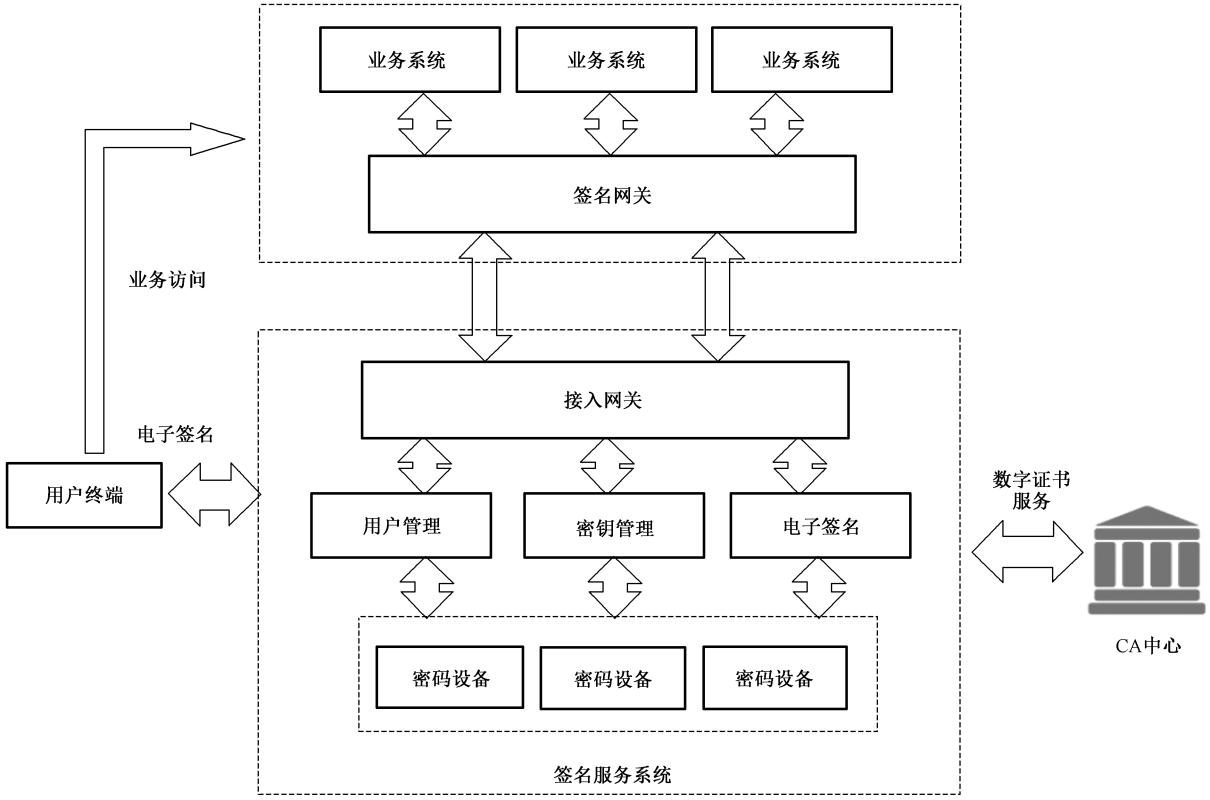

图 B.1 签名服务中心系统架构

在系统中，主要包含以下内容。

a) 签名服务系统：签名服务系统用于提供用户管理、密钥管理、数字证书管理和电子签名等功能，其内部部署多台密码设备集群，通过接口网关的转发对外提供服务。

b) 签名网关系统：签名网关系统是签名服务系统的入口。部署在业务应用的网络区域内，向业务系统提供基于通信报文或接口 SDK 的集成方式，签名网关系统将签名和证书请求经过安全保护后转发到签名服务系统处理。

c) 用户终端应用程序：用户终端应用程序提供业务的操作界面，其中集成数组签名的 SDK。SDK 提供签名密钥客户端分量的产生、存储和计算能力，提供连接到签名服务系统完成电子签名的功能。

B.3 密钥体系设计

签名服务系统中，用户电子签名所需的数字签名密钥由服务端分量和客户端分量两部分组成，这两个密钥分量都采用256位SM2算法。具体内容如下。

a) 服务端分量。用户密钥的服务端分量在硬件密码设备中产生，通过密钥加密密钥KEK加密后存储在密钥库中。在需要为特定用户进行签名时，将待签名信息、加密后的签名密钥服务端分量、加密后的KEK，送入硬件密码设备，设备首先使用设备密钥在设备内部解密KEK，再使用KEK解密服务端分量，使用此密钥分量进行协同签名。

b) 客户端分量。签名密钥的客户端分量通常采用签名方所持有的设备信息（包括但不限于IMEI、IMSI、CPU序列号等硬件信息）、用户设定的PIN码以及随机盐值通过一系列计算得到。

客户端分量不直接存储在手机端，手机端在应用沙箱内存储初始化时产生的随机信息。在需要使用客户端密钥分量进行数字签名时，再次收集设备信息，要求用户输入PIN，重新计算客户端分量，使用协同数字签名算法进行签名。

B.4 数字签名设计

数字签名过程设计如下：

a) 用户使用移动终端访问业务系统；

b) 业务系统推送签名摘要给签名访问系统，要求为特定用户或符合要求的用户完成签名；

c) 签名服务系统经过策略判断后发送签名任务给终端，在终端显示界面要求用户签名；

d) 用户通过智能手机确认，进行协同签名的部分运算；

e) 签名服务系统经过策略判断，如果策略通过则完成协同签名，合成最终签名结果；

f) 签名服务系统返回最终签名和证书。

B.5 服务设计

签名服务系统的各种功能，通过统一的接入网关，以HTTPS/JSON方式向外提供服务。服务包括用户注册、用户激活、电子签名。

业务应用通过部署认证网关，访问签名服务系统，请求签名服务系统为指定地用户或符合特定策略要求地用户进行电子签名。

用户终端通过移动互联网访问签名服务系统，按照业务系统的要求确认电子签名。

附 录 C
（资料性）
典 型 部 署

协同签名服务可采用集中部署或分部署部署，集中部署如图 C.1 所示，分布式部署如图 C.2 所示。

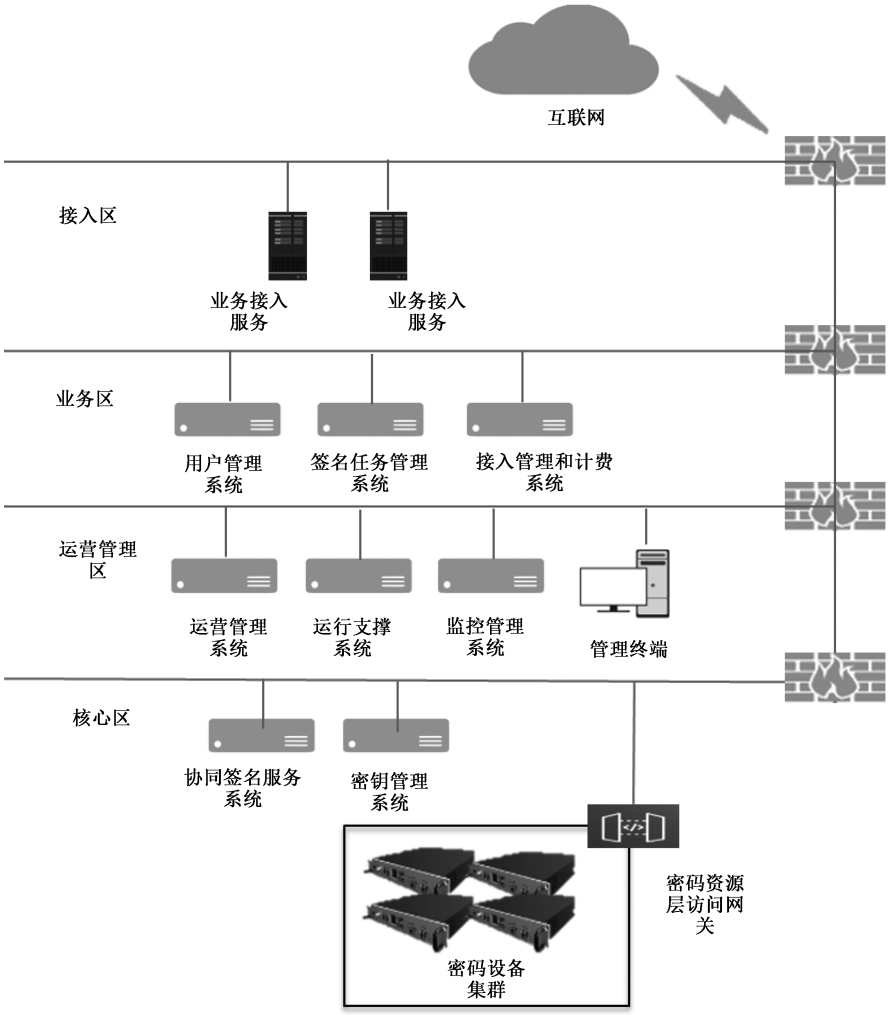

图 C.1 典型集中式协同签名服务部署示意

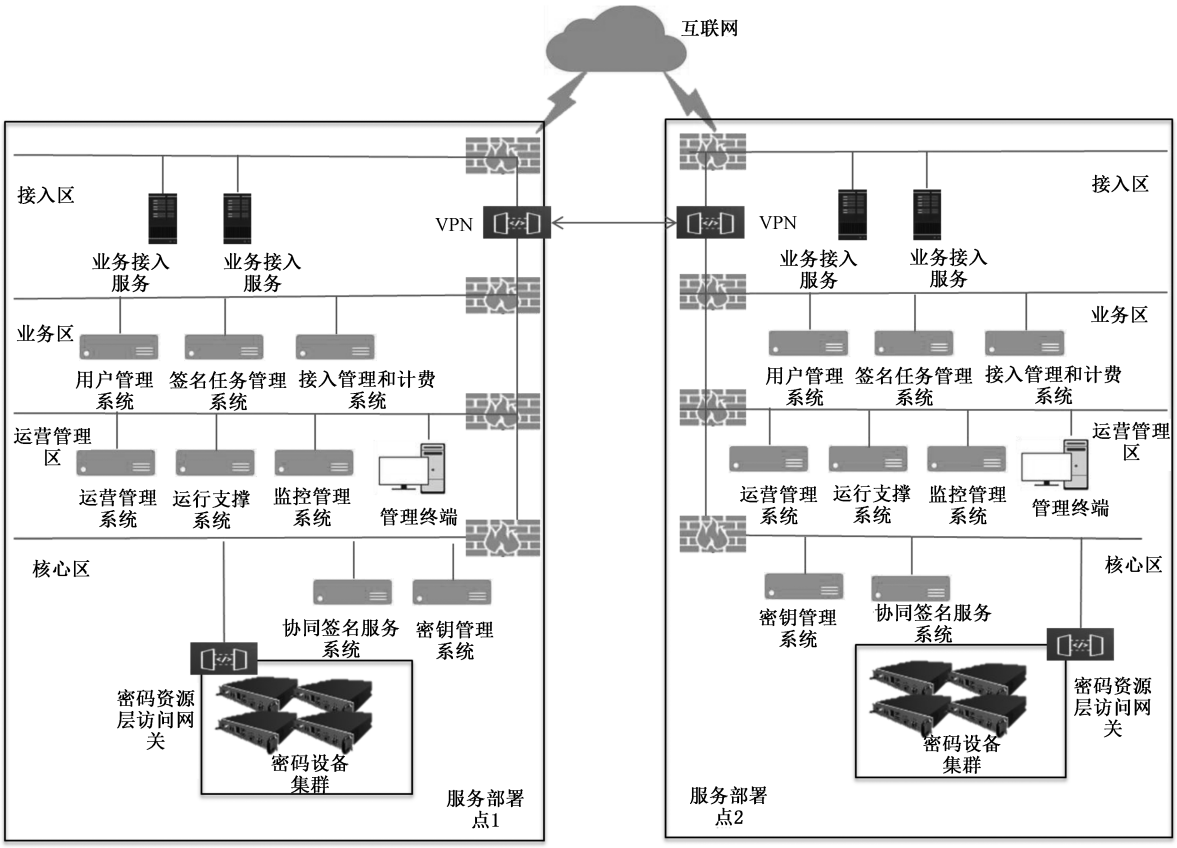

图 C.2　典型分布式协同签名服务部署示意