ICS 35.040
CCS L 80

GM

中华人民共和国密码行业标准

GM/T 0095—2020

电子招投标密码应用技术要求

Technical requirements for applications of cryptography in electronic bidding

2020-12-28 发布　　2021-07-01 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、广州公共资源交易中心、天地融科技股份有限公司、中国电力科学研究院有限公司、上海市数字证书认证中心有限公司、数安时代科技股份有限公司、中金金融认证中心有限公司、杭州天谷信息科技有限公司、吉大正元信息技术股份有限公司。

本文件主要起草人：詹榜华、田景成、杨玉奇、赵兵、林雪焰、李向锋、张永强、蓝虹、郭晓栋、李明、牟宁波、翟峰、程亮、赵丽丽、陈伟毅。

电子招投标密码应用技术要求

1 范围

本文件规定了密码技术在电子招投标业务中的应用技术要求，包括在电子招投标过程中，使用密码算法、密码产品的技术要求。

本文件适用于指导电子招投标系统中密码子系统的设计、实现和使用，电子招投标系统中密码子系统的测试、管理也可参照使用。

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 20518 信息安全技术 公钥基础设施 数字证书格式

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

GM/T 0031 安全电子签章密码应用技术规范

GM/T 0054 信息系统密码应用基本要求

GM/Z 4001—2013 密码术语

3 术语和定义

GM/Z 4001—2013 界定的以及下列术语和定义适用本文件。

3.1

非对称密码算法 asymmetric cryptographic algorithm

加解密使用不同密钥的密码算法。其中一个密钥（公钥）可以公开，另一个密钥（私钥）必须保密。由公钥求解私钥在计算上是不可行的。

3.2

数字证书 digital certificate

由证书认证机构（CA）签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及扩展信息的一种数据结构。

注 1：数字证书也称公钥证书。

注 2：按类别可分为个人证书、机构证书和设备证书，按用途可分为签名证书和加密证书。

3.3

证书认证机构 certificate authority；CA

对数字证书进行全生命周期管理的实体。

注：证书认证机构也称电子认证服务机构。

3.4

机密性　confidentiality

保证信息不被泄露给非授权的个人、进程等实体的性质。

3.5

数据完整性　data integrity

数据没有遭受以未授权方式所作的更改或破坏的特性。

3.6

抗抵赖性　non-repudiation

证明一个已经发生的操作行为无法否认的性质。

注：抗抵赖性也称不可否认性。

3.7

数字签名　digital signature

签名者使用私钥对待签名数据的杂凑值做密码运算得到的结果，该结果只能用签名者的公钥进行验证，用于确认待签名数据的完整性、签名者身份的真实性和签名行为的抗抵赖性。

3.8

电子签章　digitally seal

使用电子印章签署电子文件的过程。

3.9

电子印章　digital stamp

一种由制作者签名的包括持有者信息和图形化内容的数据，可用于签署电子文件。

3.10

时间戳　time stamp；TS

对时间和其他待签名数据进行签名得到的数据，用于表明数据的时间属性。

3.11

密钥管理　key management

根据安全策略，对密钥的产生、分发、存储、更新、归档、撤销、备份、恢复和销毁等密钥全生命周期的管理。

3.12

密钥撤消　key revocation

密钥在生存期内被撤销而失效。

3.13

密码设备　cryptographic device

能够独立完成密码服务功能的设备。

3.14

智能密码钥匙　cryptographic smart token

实现密码运算、密钥管理功能，提供密码服务的终端密码设备，一般使用 USB 接口形态。

3.15

服务器密码机　cryptographic server

能独立或并行为多个应用实体提供密码服务和密钥管理的设备。

注：服务器密码机也称主机加密服务器。

4 缩略语

下列缩略语适用于本文件。

CRL:证书撤销列表(Certificate Revocation List)

IC:集成电路(Integrated Circuit)

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

PKI:公钥密码基础设施(Public Key Infrastructure)

5 参考模型

电子招投标系统使用包括密码在内的各种安全技术来保障招投标业务安全。在电子招投标系统,对于物理和环境安全、网络和通信安全、设备和计算安全,应遵循 GM/T 0054 对信息系统的要求,对应用和数据安全,应按照电子招投标的业务过程包括用户注册、招标方案、投标邀请、发标、投标、开标、评标、定标、异议、监督、招标异常、归档进行针对性设计。电子招投标业务过程见附录 A。

电子招投标系统密码应用参考模型如图 1 所示。

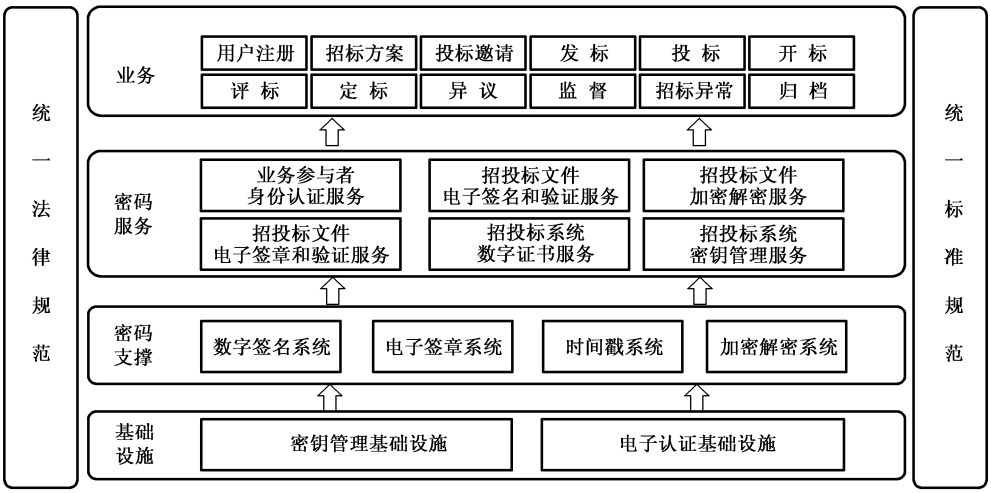

图 1 电子招投标密码应用参考模型

电子招投标系统密码应用参考模型是以密码技术为基础建立的安全服务体系,提供真实性、机密性、完整性和抗抵赖等密码服务,形成完整的安全支撑体系,以保护电子招投标业务的安全。

电子招投标系统密码应用参考模型以法律法规和标准规范为指引,划分为电子招投标业务层、密码服务层、密码支撑层、基础设施层。其功能划分如下:

a) 业务层

业务层指电子招投标业务系统,在其招投标业务的各个过程中,使用业务支撑层提供的服务,完成电子招投标的业务。

b) 密码服务层

密码服务层综合使用密码基础设施提供的密码功能,为业务层提供一系列综合性的密码服务,包括对业务参与者的身份认证服务、对招投标文件的电子签名和验证服务、对招投标文件的加密解密服务、对招投标文件的电子签章和验证服务、电子招投标系统数字证书服务、电子招投标系统密钥管理服务等。

c) 密码支撑层

密码支撑层包括向电子招投标业务系统提供密码服务的各种密码系统，包括数字签名系统、电子签章系统、时间戳系统、加密解密系统等。

d) 基础设施层

基础设施层包括在电子招投标系统中所使用的密码基础设施和电子认证基础设施，提供密钥管理服务和电子认证服务。

其中，电子认证服务应由获得主管机构许可的电子认证机构提供。

6 电子招投标业务过程密码应用要求

6.1 用户注册

在注册过程中，应对过程涉及的招标人、招标代理机构、投标人的重要敏感信息在传输过程中进行加密保护，加密应采用国家密码管理主管部门核准的密码算法。在注册过程中，应绑定合法的电子认证机构签发的数字证书。数字证书相关的要求应遵循 7.8 的要求。

此处所指敏感信息见《电子招投标系统技术规范》6.2、6.3、6.4 中的规定。

6.2 招标方案

招标方案阶段，招标方以机构名义所发布的文档，包括招标委托合同和招标项目文档，应使用招标方或代理机构的数字证书进行电子签名，宜同时使用电子签章。相关方收到文件，应检验电子签名和电子签章的有效性。电子签名及验证应遵循 7.5 的要求。电子签章及验证应遵循 7.6 的要求。

6.3 投标邀请

投标邀请阶段，电子招投标系统应使用招标方或代理机构的数字证书，对采购招标公告、资格预审公告和投标邀请书等文件进行电子签名，宜同时加盖时间戳，宜同时使用电子签章。相关方收到文件，应检验电子签章、电子签名和时间戳的有效性。

如果需要投标方出具接收回执，投标方应按照业务过程要求，向招标方提供所要求的回执。提交回执之前应对其进行电子签名。

招标方接收到投标方提交的回执后，应验证其电子签名，确认投标方已收到所发出的文档或按照要求进行了回应。

电子签名及验证应遵循 7.5 的要求。电子签章及验证应遵循 7.6 的要求。

6.4 发标

发标过程中，招标方应对所发布的文档进行电子签名并加盖时间戳，宜同时使用电子签章。招标文档可包含招标公告、招标变更公告、招标文件、招标变更/补充文件、资格预审变更/补充公告、踏勘现场通知、文件澄清答疑、文件澄清说明、下载回执等。

投标方接收到相应文档后，应验证文档的电子签名和时间戳，并按照业务过程要求，向招标方提供所要求的文档，包括公告文档接收回执和文件澄清问题等。提交文档之前应对其进行电子签名。

招标方接收到投标方提交的回执和文档后，应验证文档的电子签名，确认投标方已收到所发出的文档或按照要求进行了回应。

电子签名及验证应遵循 7.5 的要求。

6.5 投标

投标过程中，投标方应对原始投标文档包括资格预审文档、申请文件和投标文件进行电子签名，宜

同时加盖电子签章。

投标方在提交投标文档之前，应按照招标文档约定的方式，对投标文档进行加密。电子招投标系统应考虑到在投标和开标期间，可能会发生投标方用于解密的密码介质和设备损坏、丢失、过期等情况，应设计用于应急补救的方案，并与投标方达成一致。

投标过程中，电子招投标系统接收到投标方提交的密文数据，包括资格预审文档、申请文件和投标文件，同时说明数据的基本信息包括文件数量、数据描述等，电子招投标系统应在不解密数据的情况下对密文数据以及相关说明进行初步验证，并出具回执，向投标方说明接收到文档的时间点、文档数量、文档描述等信息。在发送回执前，需要对回执进行电子签名和时间戳。

投标方接收到回执信息，应验证招标方在回执中的电子签名信息和时间戳，确认回执信息的来源、完整性和不可否认性，并确认回执信息是否与所提交的投标文档情况完全一致，来保证招标方的确接收到了所提交到的文档。

电子签名及验证应遵循 7.5 的要求。投标文档加密应遵循 7.4 的要求。

6.6 开标

开标过程中，招标方和投标方应在开标时间点对投标方所提交的投标文档进行解密，系统应验证投标文档的数字签名和电子签章。如果在开标时发生介质丢失、损坏导致无法解密的情况下，应按照双方约定的应急补救方式处理。

开标过程中，系统应对开标记录进行电子签名。

电子签名及验证应遵循 7.5 的要求。电子签章及验证应遵循 7.6 的要求。

6.7 评标

评标过程中，电子招投标系统应对评标专家的身份进行认证。身份认证应遵循 7.3 的要求。

评标过程中，评标专家应能够对澄清问题、应答回执、评标报告、评标表格等电子数据进行电子签名。

投标方应能够对评标专家给出的澄清问题等文档验证电子签名，并对评标过程需要给出的应答、澄清和补充文档进行电子签名，并提交给电子招投标业务系统。

评标过程中，系统应验证投标方的应答、澄清和补充文件中的电子签名，以保证信息和文档的完整性和不可抵赖性。

电子签名及验证应遵循 7.5 的要求。

6.8 定标

定标过程中，招标方应能够对所公布的中标候选人公告、中标结果公示、中标通知书/资格预审结果/招标结果通知书进行电子签名，宜使用电子签章，可加盖时间戳。

投标方应能够对招标方公布的文档验证电子签名和时间戳。

招标方和投标方应能够通过电子招投标业务系统对中标合同进行电子签名、宜同时使用电子签章，可同时加盖时间戳，并同时验证对方的电子签名、电子签章和时间戳。

电子签名及验证应遵循 7.5 的要求。

6.9 异议

投标人对资格预审文件、招标文件、开标过程、资格预审结果、评标结果提出异议的，应对提交的异议内容进行电子签名。招标人应对答复异议的内容进行电子签名，并加盖时间戳。电子签名及验证应遵循 7.5 的要求。

6.10 监督

在向监督部门交换监督数据时，电子招投标系统应对监督数据进行电子签名。这些数据包括但不限于招标人和招标项目的基本情况、资格预审公告、招标公告、投标邀请书、资格预审文件、招标文件、资格审查委员会名单、资格预审结果报告、开标记录、评标委员会名单、评标报告、中标候选人、中标候选人公示和中标结果、合同和履行信息、招标异常信息等。电子签名及验证应遵循 7.5 的要求。

6.11 招标异常

招标人应对招标终止公告进行电子签名，在重新发布招标公告或资格预审公告、资格预审文件或招标文件时也应进行电子签名。电子签名及验证应遵循 7.5 的要求。

6.12 归档

电子招投标系统在归档时，应对招标投标数据和文件、活动记录进行电子签名，并加盖时间戳。电子签名及验证应遵循 7.5 的要求。

7 电子招投标密码应用技术要求

7.1 算法要求

电子招投标系统应使用的密码算法包括 SM3 密码杂凑算法、SM4 分组密码算法、SM2 椭圆曲线公钥密码算法。其中，SM3 密码杂凑算法应遵循 GB/T 32905，SM4 分组密码算法应遵循 GB/T 32907，SM2 椭圆曲线公钥密码算法应遵循 GB/T 32918 和 GB/T 35276。

电子招投标系统在选择密码算法时需要考虑所需密码算法强度要求、性能要求以及所涉及实体的计算能力限制等因素。

7.2 密码设备要求

7.2.1 概述

电子招投标系统所使用的密码设备分为客户端密码设备和服务端密码设备，密码设备应取得国家密码管理主管部门所颁发的资质证书。

7.2.2 客户端设备

电子招投标系统的客户端应使用智能密码钥匙、IC 卡等设备提供客户端的密码运算和密钥管理，设备应取得国家密码管理主管部门所颁发的资质证书，并在安全环境中完成初始化。

7.2.3 服务端设备

电子招投标系统应使用服务端密码设备，例如服务器密码机、签名验签服务器、时间戳服务器、密码卡等密码设备提供服务端的密码运算、证书管理和密钥管理，这些密码设备均应取得国家密码管理主管部门所颁发的资质证书，部署于安全可靠环境中，其功能、性能均应满足电子招投标系统的指标要求。

7.3 身份认证技术要求

电子招投标系统应识别每个访问实体的真实身份，明确访问实体的访问控制权限，并保证每个实体只能按照系统设定的范围使用系统提供的功能。在访问实体被成功鉴别之前，电子招投标系统应禁止执行代表该访问实体的任何操作。

电子招投标系统应建立统一的身份认证系统，基于 PKI/CA 技术实现以数字证书为核心的安全身份认证机制。招标人、招标代理机构、投标人、授权评标专家等用户应使用数字证书完成身份认证。

用户登录应使用数字证书，证书登录应进行数字签名验证和证书有效性认证，过程包括：

a) 每次登录认证是基于随机数的签名和验证，防止重放攻击；

b) 验证用户证书的信任链；

c) 验证用户证书有效期；

d) 验证证书是否被吊销。

7.4 数据加密技术要求

电子招投标系统应保证数据的机密性。数据机密性保证敏感数据不被泄露或非授权使用，包括存储机密性与传输机密性。数据的范围请参见第 6 章所描述的业务过程密码应用要求。

存储机密性是指电子招投标系统在存储敏感数据时，采用加密技术，防止敏感数据的泄露和对数据的非法访问。

传输机密性是指当访问实体访问电子招投标系统时，应采用加密传输技术，以防止传输过程中的数据泄露。

数据加密时应采用对称算法和非对称算法相结合的方式。密文数据应安全存储在数据库或磁盘上。

数据解密时，应使用数字证书对应的密码设备或证书介质解密。

数据加密可采用 GB/T 35275 中规定的加密数据格式。

7.5 电子签名技术要求

电子招投标系统应通过基于数字证书的电子签名技术保证数据电文的完整性、不可抵赖性。电子签名应符合国家相关技术规范。对于文档的签名，宜使用公开标准版式文件。

电子签名应使用可信时间对需要电子签名的数据电文生成时间戳。时间戳应符合国家相关技术规范。

数据完整性保证数据不被篡改、删除、插入和重用，包括存储完整性与传输完整性。当访问实体使用电子招投标系统提供的功能时，电子招投标系统应确保业务数据是完整的，并且在生成以后不被篡改。

招投标的参与方在进行招投标文件传输和招投标信息确认时，应采用数字签名技术来保证数据的完整性和不可抵赖性。在对电子签名进行验证时，应验证证书的有效性，包括信任链、有效期和是否被吊销。

招标投标的各方在进行重要操作时，应对招标投标文件的确认信息进行数字签名。

电子签名应采用 GB/T 35275 中规定的数字签名数据格式。

7.6 电子签章

电子招投标系统应采用电子签章等形式，对第 6 章提出需要签章的各类文档以及业务中需要签章的其他文档进行电子签名，具体请参见第 6 章业务过程的密码应用要求。电子招投标系统在使用电子签章进行签名时，电子签章的产生和使用应遵循 GM/T 0031。对电子签章的验证，也应同时验证证书的有效性，包括信任链、有效期和吊销列表。

7.7 密钥管理要求

7.7.1 密钥管理安全的目标

密钥的安全性是招投标行业数据安全的基础，电子招投标系统中使用多种密钥，包括参与电子招投

标活动各类实体的身份密钥、用以实体和系统电子签名的密钥、用以加密数据电文和通信数据的加密密钥等，其密钥管理的具体要求为：

a） 密钥的生成和使用应在硬件密码设备中完成；

b） 密钥的生成和使用应有安全可靠的管理机制；

c） 密钥应有安全可靠的备份恢复机制。

7.7.2 密钥生命周期管理

从密钥的产生和存储的方式来划分，电子招投标系统使用的密钥，可以分为保存在智能密码钥匙中的密钥和保存在服务端硬件密码设备中的密钥。保存在智能密码钥匙中的密钥又划分为签名密钥和加密密钥。密钥管理生命周期管理要求包括：

a） 密钥生成

所有的密钥（包括对称密码和非对称密钥）应由硬件密码设备生成。

b） 密钥存储

密钥应在硬件密码设备中存储。

c） 密钥使用

应用中所执行的密码运算，应由硬件加密设备在内部完成。

d） 密钥更新

存储在智能密码钥匙中的签名密钥和加密密钥应按照电子认证服务的要求进行更新，更新操作应遵循电子认证服务策略的要求。

e） 密钥备份恢复

密钥应进行定期备份，当硬件密码设备出现故障时可以进行密钥恢复。密钥备份和恢复操作由硬件设备的密钥管理工具进行，且需要多个密钥管理员同时在场执行。备份或恢复密钥时，要有满足密钥备份或恢复所必需的分管者人数要求。各个分管者输入各自的口令和分管的密钥成分，在密码设备中备份或恢复。密钥备份时管理员保管的密钥采用多人门限方式进行处理。

存储在智能密码钥匙中的加密密钥的恢复应遵循电子认证服务策略的要求。

7.8 证书管理要求

7.8.1 证书管理安全的目标

证书管理安全性的目标是保证证书在签发、使用中的安全可靠。其主要内容有：

a） 保证证书签发的可审计；

b） 防止非法签发或越权签发证书；

c） 保证证书的完整归档及归档文件的安全性；

d） 保证 CA 签名证书更新时的平稳过渡；

e） 保证 CA 机构能够对资信严重下降的用户取消其证书；

f） 防止作废证书被非法使用。

7.8.2 证书分类

电子招投标系统所采用的数字证书从所有者来区分，包括个人证书和机构证书等。

从用途角度可分为签名证书和加密证书。签名证书只用于数字签名，以保证数据的完整性和不可抵赖；加密证书用于数据加密，以保证数据的机密性保护。

7.8.3 证书认证机构

电子招投标系统应采用合法的数字证书，包括第三方电子认证机构和电子招投标系统主管部门认可的认证机构颁发的数字证书。电子招投标系统应支持多家机构的数字证书。

7.8.4 数字证书格式

数字证书格式应遵循 GB/T 20518。

7.8.5 证书生命周期管理

7.8.5.1 证书的申请

证书用户应到指定的证书业务受理点进行身份确认，由操作员对申请者的真实身份及申请资料进行可信有效的审核和确认。

7.8.5.2 证书的更新

终端用户证书即将到期，应进行更新。可以到指定受理点进行确认，如果电子认证机构支持远程证书更新，也可以采用远程方式来进行证书更新。

7.8.5.3 证书作废

终端用户证书丢失或介质损坏等情况下，应由用户到其证书发放的业务受理点进行证书作废。受理点工作人员审核通过后，将作废信息通知 CA 认证系统。然后由 CA 认证系统根据 OCSP 和 CRL 的更新规则，更新 OCSP 查询服务器中的数据，并发布新的 CRL。

7.8.6 证书处理的可审计性

为了对证书操作进行审计，对于证书的任何处理，均作日志记录，包括证书处理数据的来源、处理结果、操作人、处理后的数据去向等。通过对日志文件的统计分析，可以对证书事件进行审计和追踪。

7.9 应急补救要求

7.9.1 概述

在电子招投标过程的开标阶段中，如果发生如投标方介质损坏、丢失或过期等情况，可以采用电子招投标系统的应急补救措施进行处理。附录 B 中给出了应急补救方案的示例。应急补救措施应满足授权使用、时间限制和审计的要求。

7.9.2 应急补救措施的授权使用

应急补救措施的启动，需要严格的授权鉴别才能使用。应拥有授权权限的角色，使用数字证书登录系统，进行明确的授权。可根据实际情况，采用多人授权方案。

7.9.3 限制使用应急补救措施的时间

电子招投标系统应限制应急补救措施只能在电子招投标的开标过程，其余时间均不能使用应急补救措施。

7.9.4 审计

电子招投标系统应对应急补救措施的使用情况记录详细的日志，并进行审计。

附 录 A
（资料性）
典型电子招投标业务流程示例

电子招投标系统根据业务需要设计其业务流程，按照《电子招投标系统技术规范》，完整的电子招投标业务过程包含用户注册、招标方案、投标邀请、发标、投标、开标、评标、定标、异议、监督、招标异常、归档等过程。图 A.1 是一个典型的电子招投标业务过程示意，在实际业务系统中还包含可选过程如投标邀请、异议以及作用于整个过程的监督等。

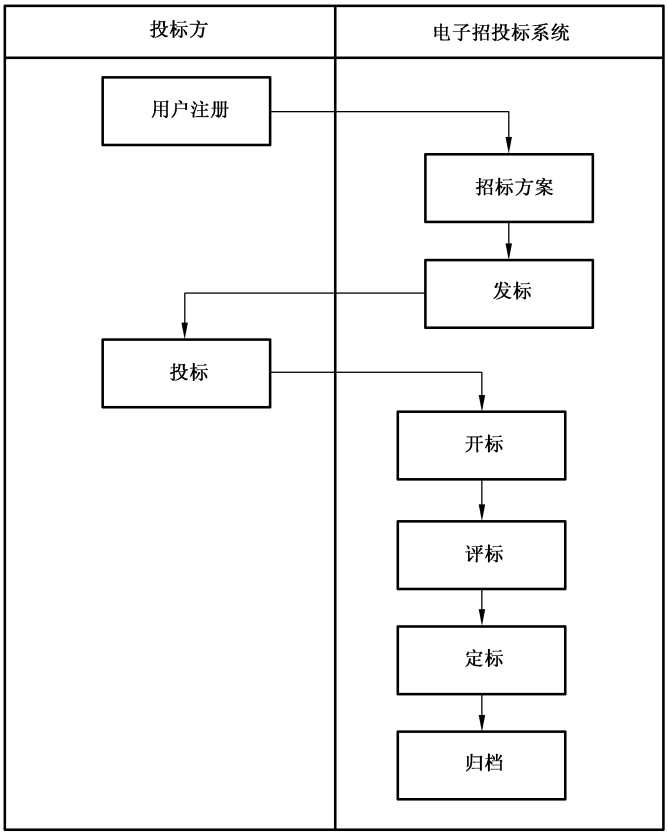

图 A.1 电子招投标业务流程

附 录 B
（资料性）
应急补救方案示例

在电子招投标的投标活动中，为了保证投标内容的数据加密要求，一般情况下，投标方用自己持有的加密证书，按照 GB/T 35275 中规定的加密数据格式，对投标内容进行加密。这样，在开标时，投标方可以在电子招投标系统中，使用自己持有的解密证书的机制，对密文进行解密。

在这种情况下，如果在开标时，发生用户解密介质（例如智能密码钥匙）损坏、丢失等情况，会导致电子招投标业务无法顺畅进行。因此在 6.6“开标”过程中，提出“应设计用于应急补救的方案”，在发送这类情况时，进行应急处理，保证业务连续性。

一种典型的参考应急补救方案是在用户投标时，除使用投标方自身加密证书对投标内容进行加密外，还使用电子招投标系统提供的一个“应急证书”的公钥进行加密，加密数据格式也符合 GB/T 35275 中规定的加密数据格式。

该加密证书由电子招投标系统在开始一个电子招投标项目时产生，在投标时使用其公钥进行对投标内容进行加密操作，仅在开标过程发生因介质故障等原因无法正常开标时，才使用“应急证书”的私钥完成解密操作。在招投标项目结束后停用归档。

系统应严格控制该应急证书的使用，包括：

a） 使用时间限制：密钥应仅在开标时间使用；

b） 使用授权：应对该密钥的使用进行权限控制，具备相应的权限才能启用该密钥；

c） 使用审计：应急密钥的使用应记录日志，包括使用应急密钥的时间、原因以及授权信息，并包含授权人的签名信息。对这些日志信息应进行严格审计，包括验证授权人的数字签名。通过这些手段严格控制该密钥的使用。

另外一种可以参考的方法是在投标时，在投标过程中，将对原始投标文件的数字签名信息随密文投标文件一起提交给电子招投标系统。如果开标时确实发生介质损坏或丢失带来的无法解密投标文件的状况，投标方可以单独再提供一份原始投标文件。电子招投标系统应检查新提供的文件是否与投标时提交的签名值匹配，如果能够匹配，可以认为两者是一致的。

参 考 文 献

[1] 中华人民共和国电子签名法(第十三届全国人民代表大会常务委员会第十次会议修订 2019 年)
[2] 电子招投标系统技术规范(中华人民共和国国家发展和改革委员会 2013 年)

中华人民共和国密码
行业标准
电子招投标密码应用技术要求
GM/T 0095—2020
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)68533533 发行中心:(010)51780238
读者服务部:(010)68523946
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 1.25 字数 29 千字
2021年4月第一版 2021年4月第一次印刷
*
书号:155066·2-35902 定价 18.00 元

GM/T 0095-2020

码上扫一扫 正版服务到