中国招标公共服务平台有限公司
China Tendering Public Service Platform Co.,ltd

电子招标投标系统技术规范

第 2 部分：公共服务平台技术规范

投标开标保障服务接口规范

（征求意见稿）

2015 年

前言

本规范依据《中华人民共和国招标投标法》、《电子招标投标办法》、《电子招标投标系统技术规范》给出的规则制订。

本规范主要起草单位：中国招标公共服务平台有限公司。

本规范技术验证单位：

目录

1 范围 3
2 规范性引用文件 3
3 术语和定义 3
3.1 对称密钥 secret key 3
3.2 非对称密码算法/公钥密码算法 3
3.3 非对称密钥对 asymmetric key pair 4
3.4 服务器密码机 cryptographic server 4
3.5 公钥 public key 4
3.6 公钥基础设施 public key infrastructure（PKI） 4
3.7 加密 encipherment/encryption 4
3.8 加密公钥 public key for encryption 4
3.9 加密私钥 private key fordecryption 4
3.10 解密 decipherment/decryption 5
3.11 密文 ciphertext 5
3.12 明文 plaintext 5
3.13 时间戳 time stamp(TS) 5
3.14 时间戳机构 time stamp authority(TSA) 5
3.15 时间戳系统 time stamp authority system 5
3.16 时间戳协议 time stamp protocol（TSP） 5
3.17 数字签名 digital signature 5
3.18 数字证书 digital certificate 6
3.19 私钥 private key 6
3.20 数字信封 digital envelope 6
3.21 SSL 协议 secure socket layer protocol 6
4 投标开标保障服务总体说明 6
5 投标开标保障服务接口说明 7
5.1 投标开标保障服务接口概述 7
5.2 生成国家平台数字信封函数定义 8
5.3 校验国家平台数字信封完整性函数定义 10
5.4 校验对称密钥完整性函数定义 11
5.5 校验是否开通投标开标保障服务函数定义 11
5.6 补救申请函数定义 12
6 接口方式规范描述 14
6.1 Com 组件调用方式规范描述 14
6.2 服务器端调用方式规范描述 14
6.3 WebService 调用方式规范描述 14
7 接口错误码对照表 15

1 范围

本规范规定了电子招标投标交易平台接入中国招标投标公共服务平台投标开标保障服务的接口规范。

适用于电子招标投标交易平台与中国招标投标公共服务平台投标开标保障服务对接程序的开发、检测、实施。

2 规范性引用文件

以下标准的相关条款通过引用而成为本规范的内容。凡是加注日期的引用文件，其随后所有的修改或修订版（勘误的内容除外）均不适用于本规范，但鼓励根据本规范达成协议的各方经协商一致适用以下标准的修订版本。凡是未加注日期的引用标准，其修订版本应自动适用于本规范。

《电子招标投标系统技术规范（第 1 部分：交易平台技术规范）》

《电子招标投标系统检测技术规范》

GB/T7408-2005 信息交换日期和时间表示法

GB/T18793-2002 信息技术可扩展标记语言（XML）

3 术语和定义

除采用《电子招标投标系统技术规范 第 1 部分：交易平台技术规范》的定义外，本规范还采用了下列专门的术语和定义。

3.1 对称密钥 secret key

用于对称密码算法的密钥。

3.2 非对称密码算法/公钥密码算法

asymmetric cryptographic algorithm/public key cryptographic algorithm

加密和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，且由公钥求解私钥是计算不可行的。

3.3 非对称密钥对 asymmetric key pair

非对称密码算法中相关联的公钥和私钥。

3.4 服务器密码机 cryptographic server

又称主机加密服务器，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。

3.5 公钥 public key

非对称密码算法中可以公开的密钥。

3.6 公钥基础设施 public key infrastructure（PKI）

基于公钥密码技术实施的具有普适性的基础设施，可用于提供机密性、完整性、真实性及抗抵赖性等安全服务。

3.7 加密 encipherment/encryption

对数据进行密码变换以产生密文的过程。

3.8 加密公钥 public key for encryption

非对称密码算法中用于实现数据机密性的公钥。

3.9 加密私钥 private key fordecryption

非对称密码算法中用于实现数据机密性的私钥。

3.10 解密 decipherment/decryption

加密过程对应的逆过程。

3.11 密文 ciphertext

加密后的数据。

3.12 明文 plaintext

未加密的数据或解密还原后的数据。

3.13 时间戳 time stamp(TS)

对时间和其它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。

3.14 时间戳机构 time stamp authority(TSA)

用来产生和管理时间戳的可信服务机构。

3.15 时间戳系统 time stamp authority system

用来产生和管理时间戳的管理系统。

3.16 时间戳协议 time stamp protocol（TSP）

描述时间戳的格式及相关消息格式的协议。

3.17 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。

3.18 数字证书 digital certificate

也称公钥证书，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。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。

3.19 私钥 private key

非对称密码算法中只能由拥有者使用的不公开密钥。

3.20 数字信封 digital envelope

一种数据结构，包含用对称密钥加密的密文和用公钥加密的该对称密钥。

3.21 SSL 协议 secure socket layer protocol

一种传输层安全协议，用于构建客户端和服务端之间的安全通道。

4 投标开标保障服务总体说明

在传统招投标向电子招投标转变过程中，投标人承担了比传统招投标额外的风险和责任，其中由于投标人的非主观因素导致开标解密失败而被取消投标资格的现象较为常见，给投标人带来了巨大损失，严重影响了招标人、投标人、交易平台以及社会对电子招标投标的信心。根据《电子招标投标办法》、《电子招标投标系统技术规范》、《电子招标投标系统检测技术规范》，中国招标投标公共服务平台为投标人提供投标开标保障服务，解决因投标人非主观因素导致的开标解密失败，消除市场主体对电子招标投标的担忧，创造远程异地开标的条件，为电子招标投标的推广保驾护航。

本方案适用于采用投标人数字证书加解密模式的交易平台，以及投标人数字证书和招标人数字证书双重加解密模式的交易平台，基本程序如下：

1） 投标人通过投标文件编制工具制作投标文件，在生成投标文件密文后，将对称密钥封装在两个数字信封内；其中一个数字信封由投标人公钥封装，另外一个数字信封由国家平

台公钥封装；其中，国家平台数字信封可以随投标人数字信封上传至交易平台，也由投标人保存在本地；上传至交易平台的数字信封在上传时由交易平台校验完整性；

2） 开标时，投标人首先使用自己的 U-KEY 对自己封装的数字信封进行拆封；

3） 如果投标人拆封失败，则可以申请补救保障服务，国家平台首先对投标人是否已开通投标开标保障服务进行校验，校验成功后，如果国家平台数字信封保存在交易平台，则由交易平台将国家平台数字信封发送给国家平台；如果国家平台数字信封保存在投标人本地，则由投标人将国家平台数字信封发送给交易平台，经交易平台校验完整性后，再发送给国家平台；

4） 国家平台拆封后将对称密钥直接发送给交易平台用于解密投标文件，完成补救保障。

交易平台可根据自身情况，选择国家平台数字信封保存在交易平台或保存在投标人本地，当然也可以同时支持这两种形式，由投标人在具体项目中自行选择。

此方案的优点如下：

1） 投标文件密文非常安全，只有拿到投标人的 U-KEY 或者投标人手中的国家平台数字信封+国家平台加密机才能解开，这些涉及物理介质很难同时获取到；

2） 投标人一键补救，操作便利，交易平台集成方便。

5 投标开标保障服务接口说明

5.1 投标开标保障服务接口概述

投标开标保障服务针对实际业务提供五个开放接口，根据实际应用环境的不同大体分成三部分，分别是投标文件编制工具、交易平台服务端、国家平台服务端。其中投标文件编制工具通过调用 Com 组件的方式实现接口对接，交易平台服务端根据不同的开发语言目前提供.NET 版和 JAVA 版，通过提供公共工具包的方式实现接口对接，国家平台服务端是通过 SSL 协议调用 Web Service 接口的方式来实现接口对接，调用时通过白名单进行过滤。

接口清单如下：

序号	功能	版本	主要函数	调用主体	说明
1	生成国家平台数字信封	客户端版本(COM 组件)	CEBPUBSERVICE_Envelope	投标文件编制工具	用于投标文件编制工具生成国家平台数字信封(适用于离线客户端)
		服务器端版本(JAVA、.NET)	CEBPUBSERVICE_Envelope	投标文件编制工具	用于投标文件编制工具生成国家平台数字信封(适用于 web 方式加密投标文件)
2	校验国家平台数字信封完整性	服务器端版本(JAVA、.NET)	CEBPUBSERVICE_VerifyEnvelope	交易平台	用于投标人上传国家平台数字信封至交易平台时，交易平台校验国家平台数字信封的完整性
3	校验对称密钥完整性	服务器端版本(JAVA、.NET)	CEBPUBSERVICE_VerifyDigest	交易平台	用于校验国家平台返回到交易平台对称密钥的完整性
4	校验是否开通投标开标保障服务	WebService 版本	CEBPUBSERVICE_VerifyBidOpen	交易平台->国家平台	检验该投标人是否已开通投标开标保障服务
5	补救申请接口	WebService 版本	CEBPUBSERVICE_ApplyBidOpen	交易平台->国家平台	交易平台向国家平台发送补救申请

5.2 生成国家平台数字信封函数定义

1)客户端版本(COM 组件) CEBPUBSERVICE_Envelope

函数名：	INT CEBPUBSERVICE_Envelope(BSTR strOrgSecretCode,BSTR strOrgBidderName, BSTR strOrgBidSectionCode,BSTR strOrgOpenFileType, BSTR strOrgPlatCode,BSTR strOrgTenderFileDigest, [out, retval] BSTR* strOutDevelope, [out, retval] BSTR * strOutDevelopeDigest)
描述：	用于投标文件编制工具生成国家平台数字信封(适用于离线客户端)
调用要点：	生成投标人数字信封之后调用本接口生成国家平台数字信封，国家平台数字信

	封可以随投标人数字信封共同上传至交易平台，也可由投标人保存到本地。			
参数：				
	参数名	含义	参数选项(In/Out)	参数类型
	strOrgSecretCode	密码串	In	BSTR
	strOrgBidderName	投标人名称	In	BSTR
	strOrgBidSectionCode	标段（包）编号	In	BSTR
	strOrgOpenFileType	开启文件类型	In	BSTR
	strOrgPlatCode	交易平台标识码	In	BSTR
	strOrgTenderFileDigest	对应的投标文件包的摘要	In	BSTR
	strOutDevelope	国家平台数字信封	Out,ret	BSTR *
	strOutDevelopeDigest	国家平台数字信封摘要	Out,ret	BSTR *
返回结果：				
	返回值	含义		
	0|非 0	成功|错误码(详见 7 接口错误码对照表)		

2)服务器端版本(JAVA、.NET)CEBPUBSERVICE_Envelope

原型：	public DigitalEnvelope CEBPUBSERVICE_Envelope(byte[] strOrgSecretCode, byte[] strOrgBidderName, byte[]strOrgBidSectionCode,byte[] strOrgOpenFileType, byte[] strOrgPlatCode,byte[] strOrgTenderFileDigest)			
描述：	用于投标文件编制工具生成国家平台数字信封(适用于 web 方式加密投标文件)			
参数：				
	参数名称	含义	参数选项 (In/Out)	数据类型
	strOrgSecretCode	密码串	In	byte[]
	strOrgBidderName	投标人名称	In	byte[]
	strOrgBidSectionCode	标段（包）编号	In	byte[]
	strOrgOpenFileType	开启文件类型	In	byte[]
	strOrgPlatCode	交易平台标识码	In	byte[]
	strOrgTenderFileDigest	对应的投标文件包的摘要	In	byte[]
返回结果：	DigitalEnvelope 为自定义类型 ， 主要包括以下属性			
	属性名	含义		数据类型
	True|false	成功|失败		boolean
	strOutDevelope	国家平台数字信封		byte[]
	strOutDevelopeDigest	国家平台数字信封摘要		byte[]

5.3 校验国家平台数字信封完整性函数定义

服务器端版本(JAVA、.NET) CEBPUBSERVICE_VerifyEnvelope

函数名：	public boolean CEBPUBSERVICE_VerifyEnvelope(byte[] strOrgDevelope,byte[] strOrgDevelopeDigest,byte[] strOrgTenderFileDigest)
描述：	用于投标人上传国家平台数字信封至交易平台后,交易平台校验国家平台数字信封的完整性

参数：				
	参数名	含义	参数选项(In/Out)	数据类型
	strOrgDevelope	国家平台数字信封	In	byte[]
	strOrgDevelopeDigest	国家平台数字信封摘要	In	byte[]
	strOrgTenderFileDigest	对应的投标文件包的摘要	In	byte[]
返回结果：				
	返回值	含义		数据类型
	true|false	成功|失败		boolean

5.4 校验对称密钥完整性函数定义

服务器端版本(JAVA、.NET) CEBPUBSERVICE_VerifyDigest

函数名：	public boolean CEBPUBSERVICE_VerifyDigest(byte[] strOrgData,byte[] strOrgDigest)			
描述：	用于校验国家平台返回到交易平台对称密钥的完整性			
参数：				
	参数名	含义	参数选项(In/Out)	参数类型
	strOrgData	对称密钥	In	byte[]
	strOrgDigest	密码摘要	In	byte[]
返回结果：				
	返回值	含义		参数类型
	true|false	成功|失败		boolean

5.5 校验是否开通投标开标保障服务函数定义

函数名：	CEBPUBSERVICE_VerifyBidOpen
描述：	检验是否开通投标开标保障服务
调用要点：	当投标人上传投标文件时，交易平台调用本函数校验该投标人是否已开通投标开标保障服务。

	名称	英文名称	值域	数据类型	数据格式
	投标人代码类型	bidderCodeType	参看 3.19 主体机构代码类型	字符型	char(2)
	投标人代码	bidderCode	参看 3.20 主体机构代码	字符型	char(50)
	投标人名称	bidderName		字符型	char(100)
	版本号	version	采用组合码，编码长度为 14 位数时间戳(YYYYMMDDhhmmss)	字符型	Char(14)
	交易平台标识码	platformCode	《电子招投标系统技术规范》附录 B.3.1 交易平台标识代码；	字符型	char(11)
	名称	英文名称	值域	数据类型	数据格式
	是否开通	servFlag	true 开通|false 未开通	boolean	
	调用失败原因	servMsg	错误码，详见 7 接口错误码对照表	int	
	服务保障截止日期	servExpiryDate(YYYYMMDD)	采用组合码，编码长度为 8 位数时间戳	字符型	

5.6 补救申请函数定义

函数名：	CEBPUBSERVICE_ApplyBidOpen				
描述：	交易平台向国家平台发送补救申请				
调用要点：	当投标人申请补救保障时，由交易平台调用本函数向国家平台发送补救申请				
参数：					
	名称	英文名称	值域	数据类型	数据格式
	投标人代码类型	bidderCodeType	参看 3.19 主体机构代	字符型	Char(2)

			码类型		
	投标人代码	bidderCode	参看 3.20 主体机构代码	字符型	Char(50)
	投标人名称	bidderName		字符型	Char(100)
	国家平台数字信封	ctpspEnvelope	自由文本	字符型	
	对应的投标文件包的摘要	tenderFileDigest	自由文本	字符型	
	国家平台数字信封的摘要	ctpspEnvDigest	自由文本	字符型	
	投标人对国家平台数字信封签名	bidderEnvDigSign	自由文本	字符型	
	交易平台对国家平台数字信封签名	platEnvDigSign	自由文本	字符型	
	投标人 Mac 地址	bidderMac	自由文本，多个地址以逗号分割	字符型	
	交易平台 Mac 地址	platMac	自由文本，多个地址以逗号分割	字符型	
	版本号	version	采用组合码，编码长度为 14 位数时间戳(YYYYMMDDhhmmss)	字符型	
	交易平台标识码	platformCode	《电子招投标系统技术规范》附录 B.3.1 交易平台标识代码；	字符型	Char(11)
返回值：					

	名称	英文名称			
	是否成功	servFlag	true 成功|false 失败	boolean	
	调用失败原因	servMsg	错误码，详见 7 接口错误码对照表	int	
	国家平台提供签名	servCtpspSignStr		字符型	
	国家平台提供时间戳	servCtpspDate		字符型	
	对称密钥	servDecryptStr		字符型	
	对称密钥摘要	servDecryptDigestStr		字符型	

6 接口方式规范描述

6.1 Com 组件调用方式规范描述

Com 组件必须基于 Windows 系统，将国家平台提供的 Com 组件存放在投标文件编制工具所在系统固定位置，并将 Com 组件注册。

注：具体注册步骤详见之后给出的“投标开标保障服务对接指南”。

6.2 服务器端调用方式规范描述

JAVA 版，将国家平台提供的工具包导入项目中,根据接口函数定义调用，工具包支持 JDK1.5 以上版本。

.NET 版，将国家平台提供的公共类库导入项目中,根据接口函数定义调用，公共类库支持 Framework3.0 以上版本。

注：根据各交易平台实际情况，如有其他要求请及时提出。

6.3 WebService 调用方式规范描述

采用 WebService 方式，符合 SOAP、WDSL 和 UDDI 规范；

通信采用 SSL 协议进行双向校验，保障传输数据安全性；

国家平台采用白名单机制对请求的交易平台 IP 地址进行过滤。

注：WSDL 相关信息及规范详见之后给出的“投标开标保障服务对接指南”。

7 接口错误码对照表

错误码（十六进制）	错误码（十进制）	错误描述
0	0	生成数字信封成功
0x0001	1	生成数字信封失败
0x0002	2	数字信封与摘要不匹配
0x0003	3	对应的投标文件包的摘要不匹配
0x0004	4	传输数据异常
0x0005	5	解密失败
0x0006	6	生成摘要失败

注：当前错误码只是简单示例开发时会随情况变化、增加。