

北京市公共资源交易中心政务云资源租用 服务项目（2026年度）（第二包、第三包） 更正说明

一、项目基本信息

项目编号：11000026210200167544-XM001

项目名称：北京市公共资源交易中心政务云资源租用
服务项目（2026年度）（第二包、第三包）

二、更正信息

更正事项：招标文件

更正内容：

（一）将招标文件第五章采购需求北京市公共资源交易中心政务云资源租用服务项目（2026年度）第二包三、技术要求 2. 服务内容及要求 2.1 参数需求：

2.1 参数需求

①北京市公共资源交易平台信息系统：

序号	服务名称	服务描述	数量	单位
1	签名验证服务	面向业务系统，通过云服务的模式提供签名验签服务，由本单位的业务系统通过 API 接口直接调用本服务实现对业务数据的签名验签。	12	项/月
2	加解密服务	面向业务系统，通过云服务的模式提供加解密服务（包括对称加解密、数字信封加解密），由本单位的业务系统通过 API 接口直接调用本服务实现对业务数据的加解密。	12	项/月
3	强身份认证服务	面向业务系统，通过云的模式提供基于数字证书的强身份认证技术服务，支持 SM2 算	12	项/月

序号	服务名称	服务描述	数量	单位
		法，以 API 方式提供密码技术支持，计算资源由云端统一保障，性能 10000 次/小时。支持单独验证签名、验证签名+验证证书、单独验证证书三种应用模式，可以配合 USBKey 证书、服务器 SSL 证书完成 PC 端以及业务之间的强身份认证。		
4	时间戳服务	面向业务系统，通过云的模式提供时间戳服务，针对可能涉及法律责任认定的关键性操作，采用合规的时间戳服务，保证关键操作的不可否认性。	12	项/月
5	SSL 安全服务	面向业务系统，通过云的模式提供 SSL 安全技术支持，支持 SM2/SM3/SM4 算法，基于国密 SSL 协议构建安全通道，用户访问系统采用 https 网络传输协议，从而确保通信时的身份鉴别、通信数据的机密性和完整性。	12	项/月
6	国密远程运维服务	面向 1 个运维人员，提供国密远程运维，需采用第三方电子认证机构颁发的 SM2 算法数字证书及介质实现登录堡垒机进行身份鉴别。	12	个/月
7	密码前置服务	提供云服务接入的安全代理功能，将密码服务平台的密码服务进行能力封装，支持系统授权和访问控制、接口监控、负载均衡、限流熔断等，避免各应用服务的重复实现。	1	套/年
8	服务器证书	验证网站所有单位的真实身份的标准型 SSL 证书，通过证书颁发机构审查网站企业身份和单域名或多域名的所有权以证明申请单位是一个合法存在的真实实体。 该产品含 SM2/RSA 双证书： 1、SM2 SSL 证书支持 360、奇安信等国密浏览器；	1	张/年

序号	服务名称	服务描述	数量	单位
		2、RSA SSL 证书支持谷歌、火狐、IE 等主流浏览器。		
9	设备证书	设备证书：标识 1 个设备的网上身份，证书有效期 1 年。	1	张/年
10	个人数字证书	个人数字证书：标识 1 个用户网上身份，证书有效期 1 年。	100	张/年
11	智能密码钥匙	具备信创《商用密码产品认证证书》，符合《党政机关信创应用功能信息类产品采购名录—商用密码产品》内的技术要求，具有身份认证、加/解密、签名/验签等功能，支持 SM2、SM3、SM4 算法。	100	套/年
12	国密浏览器	具备信创《商用密码产品认证证书》，支持 SM2、SM3、SM4 算法。	100	套/年
13	接入集成服务	提供应用系统接入手写信息数字签名系统所需应用集成、开通和配置服务等。	1	个
14	手写信息数字签名系统服务	无纸化应用中实现可靠手写数字签名的服务。	1	套/年
15	手写信息数字签名板验证服务	基本信息：支持国密算法、手写签名等；支持信创环境应用。	1	年

②北京市评标专家库管理系统

序号	服务名称	服务描述	数量	单位
1	签名验证服务	面向业务系统，通过云服务的模式提供签名验签服务，由本单位的业务系统通过 API 接口直接调用本服务实现对业务数据的签名验签。	11	项/月

2	加解密服务	面向业务系统，通过云服务的模式提供加解密服务（包括对称加解密、数字信封加解密），由本单位的业务系统通过 API 接口直接调用本服务实现对业务数据的加解密。	11	项/月
3	强身份认证服务	面向业务系统，通过云的模式提供基于数字证书的强身份认证技术服务，支持 SM2 算法，以 API 方式提供密码技术支持，计算资源由云端统一保障，性能 10000 次/小时。支持单独验证签名、验证签名+验证证书、单独验证证书三种应用模式，可以配合 USBKey 证书、服务器 SSL 证书完成 PC 端以及业务之间的强身份认证。	11	项/月
4	时间戳服务	面向业务系统，通过云的模式提供时间戳服务，针对可能涉及法律责任认定的关键性操作，采用合规的时间戳服务，保证关键操作的不可否认性。	11	项/月
5	SSL 安全服务	面向业务系统，通过云的模式提供 SSL 安全技术支持，支持 SM2/SM3/SM4 算法，基于国密 SSL 协议构建安全通道，用户访问系统采用 https 网络传输协议，从而确保通信时的身份鉴别、通信数据的机密性和完整性。	11	项/月

6	国密远程运维服务	面向 1 个运维人员，提供国密远程运维，需采用第三方电子认证机构颁发的 SM2 算法数字证书及介质实现登录堡垒机进行身份鉴别。	11	个/月
7	密码前置服务	提供云服务接入的安全代理功能，将密码服务平台的密码服务进行能力封装，支持系统授权和访问控制、接口监控、负载均衡、限流熔断等，避免各应用服务的重复实现。	1	套/年
8	服务器证书	验证网站所有单位的真实身份的标准型 SSL 证书，通过证书颁发机构审查网站企业身份和单域名或多域名的所有权以证明申请单位是一个合法存在的真实实体。	1	张/年
9	设备证书	设备证书：标识 1 个设备的网上身份，证书有效期 1 年。	1	张/年
10	个人数字证书	个人数字证书：标识 1 个用户网上身份，证书有效期 1 年。	100	张/年
11	智能密码钥匙	具备信创《商用密码产品认证证书》，符合《党政机关信创应用功能信息类产品采购名录—商用密码产品》内的技术要求，具有身份认证、加/解密、签名/验签等功能，支持 SM2、SM3、SM4 算法。	100	套/年

12	国密浏览器	具备信创《商用密码产品认证证书》，支持 SM2、SM3、SM4 算法。	100	套/年
13	接入集成服务	提供应用系统接入手写信息数字签名系统所需应用集成、开通和配置服务等。	1	个

更正为：

2.1 参数需求

①北京市公共资源交易平台信息系统

序号	服务名称	服务描述	数量	单位
1	签名验证服务	面向业务系统，通过云服务的模式提供签名验签服务，由本单位的业务系统通过 API 接口直接调用本服务实现对业务数据的签名验签。	11	项/月
2	加解密服务	面向业务系统，通过云服务的模式提供加解密服务（包括对称加解密、数字信封加解密），由本单位的业务系统通过 API 接口直接调用本服务实现对业务数据的加解密。	11	项/月
3	强身份认证服务	面向业务系统，通过云的模式提供基于数字证书的强身份认证技术服务，支持 SM2 算法，以 API 方式提供密码技术支持，计算资源由云端统一保障，性能 10000 次/小时。支持单独验证签名、验证签名+验证证书、单独验证证书三种应用模式，可以配合 USBKey 证书、服务器 SSL 证书完成 PC 端以及业务之间的强身份认证。	11	项/月
4	时间戳服务	面向业务系统，通过云的模式提供时间戳服务，针对可能涉及法律责任认定的关键性操作，采用合规的时间戳服务，保证关键操作的不可否认性。	11	项/月

序号	服务名称	服务描述	数量	单位
5	SSL 安全服务	面向业务系统，通过云的模式提供 SSL 安全技术支持，支持 SM2/SM3/SM4 算法，基于国密 SSL 协议构建安全通道，用户访问系统采用 https 网络传输协议，从而确保通信时的身份鉴别、通信数据的机密性和完整性。	11	项/月
6	国密远程运维服务	面向 1 个运维人员，提供国密远程运维，需采用第三方电子认证机构颁发的 SM2 算法数字证书及介质实现登录堡垒机进行身份鉴别。	11	个/月
7	密码前置服务	提供 11 个月的云服务接入的安全代理功能，将密码服务平台的密码服务进行能力封装，支持系统授权和访问控制、接口监控、负载均衡、限流熔断等，避免各应用服务的重复实现。	1	套
8	服务器证书	验证网站所有单位的真实身份的标准型 SSL 证书，通过证书颁发机构审查网站企业身份和单域名或多域名的所有权以证明申请单位是一个合法存在的真实实体。 该产品含 SM2/RSA 双证书： 1、SM2 SSL 证书支持 360、奇安信等国密浏览器； 2、RSA SSL 证书支持谷歌、火狐、IE 等主流浏览器。 有效期 11 个月	1	张
9	设备证书	设备证书：标识 1 个设备的网上身份，证书有效期 11 个月。	1	张
10	个人数字证书	个人数字证书：标识 1 个用户网上身份，证书有效期 11 个月。	100	张
11	智能密码钥匙	具备信创《商用密码产品认证证书》，符合《党政机关信创应用功能信息类产品采购名录—商用密码产品》内的技术要	100	套

序号	服务名称	服务描述	数量	单位
		求，具有身份认证、加/解密、签名/验签等功能，支持 SM2、SM3、SM4 算法，有效期 11 个月。		
12	国密浏览器	具备信创《商用密码产品认证证书》，支持 SM2、SM3、SM4 算法，有效期 11 个月。	100	套
13	接入集成服务	提供 11 个月的应用系统接入手写信息数字签名系统所需应用集成、开通和配置服务等。	1	个
14	手写信息数字签名系统服务	无纸化应用中实现可靠手写数字签名的服务，有效期 11 个月。	1	套
15	手写信息数字签名板验证服务	基本信息：支持国密算法、手写签名等；支持信创环境应用，有效期 11 个月。	1	项

②北京市评标专家库管理系统

序号	服务名称	服务描述	数量	单位
1	签名验证服务	面向业务系统，通过云服务的模式提供签名验签服务，由本单位的业务系统通过 API 接口直接调用本服务实现对业务数据的签名验签。	11	项/月
2	加解密服务	面向业务系统，通过云服务的模式提供加解密服务（包括对称加解密、数字信封加解密），由本单位的业务系统通过 API 接口直接调用本服务实现对业务数据的加解密。	11	项/月
3	强身份认证服务	面向业务系统，通过云的模式提供基于数字证书的强身份认证技术服务，支持 SM2 算法，以 API 方式提供密码技术支持，计算资源由云端统一保障，性能 10000 次/小时。支持单独验证签	11	项/月

		名、验证签名+验证证书、单独验证证书三种应用模式，可以配合 USBKey 证书、服务器 SSL 证书完成 PC 端以及业务之间的强身份认证。		
4	时间戳服务	面向业务系统，通过云的模式提供时间戳服务，针对可能涉及法律责任认定的关键性操作，采用合规的时间戳服务，保证关键操作的不可否认性。	11	项/月
5	SSL 安全服务	面向业务系统，通过云的模式提供 SSL 安全技术支持，支持 SM2/SM3/SM4 算法，基于国密 SSL 协议构建安全通道，用户访问系统采用 https 网络传输协议，从而确保通信时的身份鉴别、通信数据的机密性和完整性。	11	项/月
6	国密远程运维服务	面向 1 个运维人员，提供国密远程运维，需采用第三方电子认证机构颁发的 SM2 算法数字证书及介质实现登录堡垒机进行身份鉴别。	11	个/月
7	密码前置服务	提供 11 个月的云服务接入的安全代理功能，将密码服务平台的密码服务进行能力封装，支持系统授权和访问控制、接口监控、负载均衡、限流熔断等，避免各应用服务的重复实现。	1	套

8	服务器证书	验证网站所有单位的真实身份的标准型 SSL 证书，通过证书颁发机构审查网站企业身份和单域名或多域名的所有权以证明申请单位是一个合法存在的真实实体。有效期 11 个月。	1	张
9	设备证书	设备证书：标识 1 个设备的网上身份，证书有效期 11 个月。	1	张
10	个人数字证书	个人数字证书：标识 1 个用户网上身份，证书有效期 11 个月。	100	张
11	智能密码钥匙	具备信创《商用密码产品认证证书》，符合《党政机关信创应用功能信息类产品采购名录—商用密码产品》内的技术要求，具有身份认证、加/解密、签名/验签等功能，支持 SM2、SM3、SM4 算法，有效期 11 个月。	100	套
12	国密浏览器	具备信创《商用密码产品认证证书》，支持 SM2、SM3、SM4 算法，有效期 11 个月。	100	套
13	接入集成服务	提供 11 个月的应用系统接入手写信息数字签名系统所需应用集成、开通和配置服务等。	1	个

(二) 将招标文件第五章采购需求北京市公共资源交易中心政务云资源租用服务项目(2026 年度)第二包三、技术要求 2. 服务内容及要求 2.2 技术参数 (一) 密码云服务:

2.2 技术参数

(一) 密码云服务

密码云服务包括强身份认证服务、签名验证服务、加解密服务、SSL 安全服务、远程运维接入服务（国密）、时间戳服务及密码前置服务。

1. 强身份认证服务

提供 1 年租赁服务。面向业务系统，通过云服务的模式提供基于数字证书的强身份认证服务，本服务支持单独验证签名、验证签名+验证证书、单独验证证书三种应用模式，本服务可以配合 USBKey 证书完成 PC 端以及业务服务之间的强身份认证。

2. 签名验证服务

提供 1 年租赁服务。面向业务系统，通过云服务的模式提供签名验证服务，基于数字签名技术对业务系统中关键数据和操作进行签名及验签。

3. 加解密服务

提供 1 年租赁服务。面向业务系统，通过云服务的模式提供加解密服务，实现对系统中重要数据的存储机密性保护。

4. SSL 安全服务

提供 1 年租赁服务。面向业务系统，通过云服务的模式提供 SSL 安全服务，基于国密 SSL 协议构建安全通道，用户访问系统采用 https 网络传输协议，从而确保通信时的身份鉴别、通信数据的机密性和完整性。

5. 远程运维接入服务（国密）

提供 1 年租赁服务。面向业务系统运维人员开通 1 个远程运维接入服务（国密）。支持 SM2/SM3/SM4 算法，针对业务系统涉及的应用服务器、数据库服务器以及数据库管理系统，基于密码技术构建国密 SSL VPN 加密通道，运维管理人员采用智能密码钥匙登录 VPN 和堡垒机，通过国密数字证书认证的方式实现身份鉴别和远程运维安全。

6. 时间戳服务

提供 1 年租赁服务。面向业务系统，通过云的模式提供时间戳服务，针对可能涉及法律责任认定的关键性操作，采用合规的时间戳服务，保证关键操作的不可否认性。

7. 密码前置服务

提供云服务接入的安全代理功能，将密码服务平台的密码服务进行能力封装，支持系统授权和访问控制、接口监控、负载均衡、限流熔断等，避免各应用服务的重复实现。

更正为：

2.2 技术参数

(一) 密码云服务

密码云服务包括强身份认证服务、签名验证服务、加解密服务、SSL 安全服务、远程运维接入服务（国密）、时间戳服务及密码前置服务。

1. 强身份认证服务

提供 11 个月的租赁服务。面向业务系统，通过云服务的模式提供基于数字证书的强身份认证服务，本服务支持单独验证签名、验证签名+验证证书、单独验证证书三种应用模式，本服务可以配合 USBKey 证书完成 PC 端以及业务服务之间的强身份认证。

2. 签名验证服务

提供 11 个月的租赁服务。面向业务系统，通过云服务的模式提供签名验证服务，基于数字签名技术对业务系统中关键数据和操作进行签名及验签。

3. 加解密服务

提供 11 个月的租赁服务。面向业务系统，通过云服务的模式提供加解密服务，实现对系统中重要数据的存储机密性保护。

4. SSL 安全服务

提供 11 个月的租赁服务。面向业务系统，通过云服务的模式提供 SSL 安全服务，基于国密 SSL 协议构建安全通道，用户访问系统采用 https 网络传输协议，从而确保通信时的身份鉴别、通信数据的机密性和完整性。

5. 远程运维接入服务（国密）

提供 11 个月的租赁服务。面向业务系统运维人员开通 1 个远程运维接入服务（国密）。支持 SM2/SM3/SM4 算法，针对业务系统涉及的应用服务器、数据库服务器以及数据库管理系统，基于密码技术构建国密 SSL VPN 加密通道，运维管理人员采用智能密码钥匙登录 VPN 和堡垒机，通过国密数字证书认证的方

式实现身份鉴别和远程运维安全。

6. 时间戳服务

提供 11 个月的租赁服务。面向业务系统，通过云的模式提供时间戳服务，针对可能涉及法律责任认定的关键性操作，采用合规的时间戳服务，保证关键操作的不可否认性。

7. 密码前置服务

提供 11 个月的云服务接入的安全代理功能，将密码服务平台的密码服务进行能力封装，支持系统授权和访问控制、接口监控、负载均衡、限流熔断等，避免各应用服务的重复实现。

