合同编号：04

西安市红会医院
密码改造信源加密项目合同

甲方：西安市红会医院

乙方：西安腾信格安数据科技有限公司

甲方：西安市红会医院（以下简称“甲方”）

乙方：西安腾信格安数据科技有限公司（以下简称“乙方”）

甲、乙双方经过平等协商，在真实、充分地表达各自意愿的基础上，根据《中华人民共和国民法典》及其他相关法律的规定，就乙方为甲方提供密码改造信源加密事宜，甲乙双方经协商一致达成如下协议，并由双方共同遵照执行。

一、合同标的物内容

1．产品名称、品牌、型号、数量及金额。

序号	货物名称	制造厂家	规格及型号	数量	单价（元）	总价（元）
1	西安市全民健康信息平台数据加密前置模块	西安腾信格安数据科技有限公司	软件/腾信云PT-1000	1	100000.00	100000.00
2	云服务器密码机	渔翁信息技术股份有限公司	2U机架式机箱、64G内存、960G硬盘、2个100/1000M的RJ45接口，2个光口10Gbps以太网光纤SFP+接口/SJJ2301-G	1	100000.00	100000.00
3	国密安全认证网关	渔翁信息技术股份有限公司	1U机架式机箱、16G内存、64G硬盘、7个千兆电口+4个千兆光口/SJJ1929-G	1	100000.00	100000.00
4	系统对接开发服务	西安腾信格安数据科技有限公司	软件/定制开发	1	83000.00	83000.00
总价		大写：人民币叁拾捌万叁仟元整；小写：¥383000.00元				

2．本合同约定的货物所有权均归甲方所有。

3．服务期限：自合同签订之日起3年。

二、合同价款

1．合同总价款为¥383000.00元（人民币：叁拾捌万叁仟元整）。

2．合同总价包括但不限于：运输费、保险费、装卸费、配套资料费、安装

调试费用、强制性第三方监督检验机构的验收检验费、培训费用以及售后服务费用及税金等所有费用等。

3. 合同总价一次性包死，不受市场价格、政府政策、不可抗力等变化因素的影响，合同履行期间，无论发生任何突发或者其他事件，甲方不再另行支付任何费用。

三、结算方式及账户信息

1. 履约保证金的收取与退回：在中标结果公示发布后5个工作日内乙方将项目履约保证金（中标总金额的5%，即19150.00元）转账至甲方基本户，未按照招标文件要求按时足额缴纳履约保证金的，甲方将取消乙方中标资格，且无需承担任何责任，甲方可重新组织招标活动。自项目验收合格后并交付使用后3年，无任何问题，甲方向乙方无息退还履约保证金。

2. 款项结算：设备到货完成平台对接并且项目验收合格（以甲方出具结论为合格的书面验收报告为准）且乙方向甲方开具相应的合法合规发票后10日内甲方向乙方支付合同总价款的90%，即¥ 344700.00元（人民币：叁拾肆万肆仟柒佰元整）；剩余10%于系统上线运行一个月后并经甲方确认（以甲方出具书面确认单为准）且乙方向甲方开具相应的合法合规发票后10日支付，即¥38300.00元（人民币：叁万捌仟叁佰元整）。若乙方延期开票的，甲方有权暂停付款，不视为违约，乙方应按照合同正常履行义务。如因甲方财务制度及付款流程等原因导致延期支付，双方友好协商解决。

3. 支付方式：银行转账。

4. 甲乙双方银行账户信息和纳税人信息如下：

甲方：西安市红会医院

开户行：[中国银行长安路支行]

银行地址：[陕西省西安市碑林区南关正街3号]

户名：[西安市红会医院]

账号：[102407334632]

统一社会信用代码：[12610100437203580Q]

地址：[西安市碑林区南稍门南郭路76号]

电话：[029-87800002]

乙方：西安腾信格安数据科技有限公司

开户行：[中国民生银行股份有限公司西安东关正街支行]

银行地址：[西安市碑林区东关正街66号世贸大厦一层]

户名：西安腾信格安数据科技有限公司

账号：[150700895]

统一社会信用代码：[91610103MA6TYDCT9W]

地址：[陕西省西安市高新区科技二路67号启迪科技园L座12A03室]

电话：[029-88810301]

上述账户信息如有变更，乙方应在合同规定的相关付款期限前二十天内以书面方式通知对方，如未按时通知 或通知有误而影响结算者，责任由责任方自负。

四、技术参数

序号	产品名称		技术参数
1	西安市全民健康信息平台数据加密前置模块	功能参数	1、可接入西安市全民健康信息平台部署的密码服务管理中台，与西安市全民健康信息平台数据采集引擎实现密钥同步功能。 2、支持密码运算单元自适应、密码服务流控管理、密钥云安全分发、密钥同步等技术,能够衔接密码设施资源池和统一密码服务，用于虚拟化密码资源的统一调度； 3、支持查看租户所拥有的密码服务，可以根据服务类型、服务名称进行搜索。 4、支持查看租户所拥有的应用信息，可以通过服务类型、应用名称进行搜索。
2	云服务器密码机	硬件参数	1、标准2U机架式设备，100/1000M的RJ45接口≥2个，光口10Gbps以太网光纤SFP+接口≥2个，采用国产8核处理器+国产主板硬件架构、内存≥64G、硬盘≥960G SSD，至少1个COM口、1个Console口、1个VGA接口及4个USB接口、国产化操作系统（带永久正版授权）、虚拟机数量≥8个； 2、SM2算法密钥生成速率≥40000对/秒；SM2算法加密速度≥50Mbps；SM2算法解

			密速度≥160Mbps；SM2 算法签名速度≥90000 次/秒；SM2 算法验签速度≥40000 次/秒；SM1 算法加解密速度≥2000Mbps；SM4 算法加解密速度≥16000Mbps；SM3 杂凑算法≥11000Mbps；
		功能参数	1、支持对称、非对称密钥管理功能，包括密钥批量生成和批量删除、密钥备份、密钥恢复等功能，支持不少于 1024 条密钥的管理能力，支持由内部密钥保护到外部密钥保护的数字信封转换，支持密钥互操作协议(KMIP)； 2、支持 VLAN 池划分，当虚拟机选择同一个 VLAN 后，只同一个 VLAN 内的虚拟机可以互相访问，与其他虚拟机无法通信； 3、支持虚拟机创建、虚拟机克隆、虚机漂移、镜像管理、虚拟机集群等功能，支持按实际需求创建不同规格与性能的虚拟机密码机，支持虚拟密码机的创建、启动、停止、删除等操作； 4、支持系统进行升级，可显示历史升级记录； 5、支持 SM1、SM4 等国密算法； 6、支持 IPV4/IPV6 双栈网络协议； 7、支持日志等级设置； 8、支持通过 SNMP 协议监控设备状态，实现反馈服务器密码机后台服务状态、业务连接数、密码 CPU、内存使用率等； 9、具备《商用密码产品认证证书》；
3	国密安全认证网关	硬件参数	1、1U 机架式机箱，国产化 8 核处理器、内存≥16G DDR4，64GB M.SATA 固态硬盘，接口≥7 个千兆电口+4 个千兆光口，国产化操作系统，至少 1 个 Console 接口、2 个电源接口、1 个电源开关、2 个 USB 接口、2 个电源指示灯、6 组网口状态指示灯和 6 个系统 LED 状态指示灯； 2、IPSec 密文吞吐率≥2000Mbps，最大并发隧道数≥1000，每秒新建隧道数≥100；SSL 密文吞吐率≥2000Mbps，每秒新建连接数≥1000tps，最大并发连接数≥20000，最大并发用户数≥2000；

		功能参数	1、支持“多因子”身份鉴别与访问控制；认证因子至少包含PIN码、二维码扫码、数字证书和口令等身份认证方式；支持统一身份认证功能，能够提供静态密码、数字证书等多种身份认证方式； 2、支持OSPF OVER IPSec，能够自动识别网络情况，适应复杂网络路由机制。支持隧道断线重连，能够定期监测网络状态，实现隧道断线自动重建； 3、至少支持SM1、SM2、SM3、SM4密码算法，国密SSL算法套件支持ECC(SM2)-SM4-SM3、ECC(SM2)-SM1-SM3算法套件；国密IPSec隧道模式支持SM2+SM1+SM3+ESP、SM2+SM4+SM3+ESP隧道模式； 4、支持SSL自适应，搭配国密和非国密浏览器，实现SSL自适应，实现数据以HTTPS形式传输；支持SSL代理WEB资源和TCP资源；应用访问协议：HTTPS 5、支持单点登录功能，各应用系统用户只需登录一次IPsec/SSL VPN管理系统，即可访问被授权使用的所有应用系统。登出后，被授权的系统均不可再执行操作； 6、支持量子密钥，支持对接量子密钥库，实现基于量子密钥的数据传输机密性保护； 7、能够展示设备运行情况，包括CPU使用情况、内存使用情况、存储使用情况等； 8、具有《商用密码产品认证证书》；

五、服务要求

1．为确保数据采集引擎与西安市全民健康信息平台数据加密前置模块的业务连续性与系统稳定性，乙方需严格遵循接口文档规范（详情见“附件1”）进行定制化代码开发。开发工作应精准匹配数据采集引擎的实际业务逻辑，最终实现系统间的无缝对接与安全集成。

2．交货期：自合同签订后45个日历日内全部交货并安装调试完毕，并交付甲方验收合格。

3．交货地点：西安市红会医院。

4．交货方式：由乙方负责配送、安装、调试、培训等。

5、乙方需要提供培训服务，对设备的操作、维修、保养等内容进行培训，确保甲方相关管理维护人员能熟练操作使用、能发现一般问题、能排除一般故障。

6、合同签订后，乙方成立由专业人员组成不少于3人的实施团队，至少包含项目经理1人、实施工程师1人、系统开发1人，医院有权根据实际情况更换项目经理或实施人员。

序号	姓名	性别	身份证	联系电话	岗位
1	程馨	女	612423199805254829	15129489936	项目经理
2	李艳艳	女	610523199607056921	15390846459	实施工程师
3	马连宇	男	371082200101220711	15550643220	系统开发

六、交付成果

提供西安市全民健康信息平台系统兼容证明；《项目验收单》；硬件设备的《产品检测报告》、《合格证》；软件系统的《计算机软件著作权登记证书》。

七、验收标准或规范

稳定运行并成功对接全民健康平台

八、产品质量保证

乙方提供的服务及备件耗材必须保证质量可靠，应全面满足谈判文件的要求，谈判文件未明确要求的内容，乙方按采购服务要求或以甲方的补充要求为准。所供服务应严格按照国家最新发布的规范标准执行，如发生问题由乙方承担全部责任。乙方要求具有完善的管理及服务体系、高效的工作作风。

九、产品质保期

1、质量保证期：自项目验收合格后并交付使用后3年。

2、乙方对提供的货物在质保期内，因产品质量而导致的缺陷，必须免费提供包修、包换、包退服务。

3、质保期内，用户在使用过程中出现的问题，乙方应当及时提供技术支持，通过 Email、电话等形式在半小时内响应用户的技术支持要求；若需现场支持，应在 48 小时内到达，1 周内处理完毕。

十、违约责任

1．按《中华人民共和国民法典》中的相关条款执行。

2．乙方未按合同要求履行合同义务，所提供设备及服务质量不能满足合同

约定的技术要求，在约定的条件下，乙方必须无条件更换，提高技术，完善质量，否则，甲方有权解除合同，解除合同书面通知书到达乙方之日视为合同已解除，并按以下三种方式追究乙方的违约责任：（1）乙方赔偿甲方解除合同的全部损失（包括但不限于重新采购产生的费用、甲方对第三方的违约损失，以及可能产生的律师费、诉讼费等全部费用）；（2）乙方支付甲方违约金，违约金计算方法：以合同总价为基数，支付甲方合同总价的30%为违约金；（3）请政府采购管理部门对其违约行为进行追究。

3．在合作期内，一方违反本合同约定，另一方可以视情况中止履行相关义务并要求违约方限期履行，待违约方在守约方规定的合理期限内履行完毕相关义务后，守约方视情况决定是否恢复履行其义务；若（1）守约方决定不再恢复本合同项下义务；（2）违约方未在限期内履行完毕其义务；（3）违约方明确表示其不再履行其义务；（4）违约方以实际行动表示不再履行其义务；守约方有权单方面解除本协议，协议自书面解除通知书到达违约方时解除。给守约方造成损失的，违约方还应当在损失范围内进行赔偿，另支付守约方合同总价款30%的违约金。本条款所指损失：包括但不限于律师费、调查取证费、差旅费、鉴定费等全部费用。

十一、争议解决

1．所有因本合同引起的或与本合同有关的任何争议通过双方友好协商解决。如果双方不能通过友好协商解决争议，则任何一方均可向甲方住所地有管辖权的人民法院起诉。

2．诉讼进行过程中，双方继续履行本合同未涉诉讼的其他部分。

十二、保密条款

1．甲乙双方均应对本合同内容保守秘密，不经对方同意不得将本合同内容泄露给第三方。由此引起的法律纠纷，由泄露方承担全部责任，且该保密义务不因本合同的终止而丧失。

2．由甲乙任何一方提供或公开标有限制使用或传播的说明或以其他方式表明是保密或者专有的所有文件、技术资料、商业信息和软件及其相关的文件，无论以何种方式记录，或是以口头或视听方式提供的，其产权归提供方所有。

十三、不可抗力

1、不可抗力是指本合同生效后，发生合同订立时不能预见、不能避免，并不能克服的客观情况，如地震、台风、水灾、战争等，致使直接影响本合同的履行或不能按约定的条件履行的情况。

2、发生不可抗力的一方应立即通知对方，并在十五天内提供不可抗力的详情及将有关证明文件送交对方，且应尽可能减少不可抗力所产生之影响。

3、发生不可抗力事件时，甲乙双方应协商以寻找合理的解决方法，双方不可放任不可抗力事件损害后果。

4、经双方确认的不可抗力影响时间，不计入本合同执行时间。本合同期限可根据中止的期限作相应延长，但须双方协商一致，任何一方均不会因此而承担责任。

5、如不可抗力事件持续三十天时，甲乙双方应友好协商解决本合同是否继续履行或终止的问题。

6、在发生不可抗力时，双方对各自控制下的设备、资料负有保管责任，对于未受不可抗力影响并且可以继续履行的合同义务应继续履行。

十四、合同生效及其他

1、在本合同执行过程中，甲乙双方协商签订的补充合同与原合同具有同等法律效力，补充合同与原合同不一致的，以补充合同为准。技术协议、采购文件及其补遗文件、投标文件和有关说明承诺（若有）是本合同不可分割的部分，为本合同的重要补充内容，与本合同具有同等法律效力。

2、除本合同另有约定外，未经甲乙双方书面确认，任何一方不得自行变更或修改本合同。

3、未尽事宜，双方协商解决。

4、本合同自双方盖章之日起生效；本合同一式伍份，甲方肆份，乙方壹份，每份具有同等法律效力。

（本页无正文，为《西安市红会医院密码改造信源加密项目》签署页）

甲方（盖章）：西安市红会医院

法定代表人或委托代理人签字：

经办人：

签订日期：2026年 2 月 9 日

乙方（盖章）：西安腾信格安数据科技有限公司

法定代表人或委托代理人签字：

签订日期：2026年 2 月 9 日

附件 1

1. 概述

本文描述了加密机JAVA API 接口的调用说明。文档的阅读对象主要为相关业务系统开发人员和设计人员。

2. 接口说明

2.1 集成方式

jar包可以通过开发工具设置引用jar包，打包至工程内。

2.2 JDK 版本

默认要求JDK版本在 1.8 以上。

3. 接口定义

BaseApi 类是一个封装了所有外部服务调用的类，以下接口需在此类实现，通过调用封装的接口实现相应功能。

3.1 打开密码设备接口

3.1.1 接口说明

设置服务器密码机ip、连接数和端口，支持多台服务器密码机ip配置打开密码设备。在使用密码设备提供的功能之前，必须首先执行打开密码设备操作。该操作完成密码设备初始化。在应用程序中只需调用打开设备一次，当所有操作完成后调用关闭设备的函数释放资源。

3.1.2 接口定义

```
public void openDevice(byte[] pass, String[] ipList, int connectNum,
int port);
```

3.1.3 输入参数

参数名称	是否必填	说明
pass	是	服务器密码机连接口令
ipList	是	服务器密码机 IP 地址，支持单台或者多台服务器密码机 ip 的配置
connectNum	是	每台服务器密码机的连接数
port	是	端口号，默认 8012，可以传其他映射端口号

3.1.4 返回参数

无。异常则直接抛出。

3.2 关闭密码设备接口

3.2.1 接口说明

关闭密码设备。在最后一次访问密码设备提供的功能之后，必须执行本操作完成系统资源的释放工作。

3.2.2 接口定义

```
public void closeDevice ();
```

3.2.3 输入参数

无

3.2.4 输出参数

无。异常则直接抛出。

3.3 对称加密接口

3.3.1 接口说明

使用指定的密钥和IV,以及指定的对称密钥分组加密算法和工作方式对输入数据进行对称加密运算（对称加密接口需至少支持 1024×1024KB的数据大小）。

3.3.2 接口定义

```
public int symEcrypt(int alg, int mode, byte[] inData, int inLen, byte[] out, int[] outLen, byte[] keyData, int keyLen, byte[] iv, int ivLen);
```

3.3.3 输入参数

参数名称	是否必填	说明
alg	是	算法标识，有效取值如下： ALG_SM1：SM1 算法； ALG_SM4：SM4 算法； ALG_AES：AES 算法； ALG_AES192：AES192 算法； ALG_AES256：AES256 算法； ALG_DES：DES 算法； ALG_3DES：3DES 算法；
mode	是	对称运算工作模式，有效值如下： ALGMODE_ECB；

		ALGMODE_CBC; ALGMODE_CFB; ALGMODE_OFB; ALGMODE_CTR;
inData	是	用于存放输入数据
inLen	是	输入数据字节长度，有效值必须是算法分组长度的整数倍； SM1、SM4：16 的倍数； DES、3DES：8 的倍数； AES、AES192、AES256：16 的倍数；
out	是	用于输出密文数据
outLen	是	用于输出密文数据的字节长度
keyData	是	用于存放输入对称密钥数据。
keyLen	是	输入密钥数据字节长度，有效值如下： SM1、SM4、AES：16； DES：8； 3DES：24； AES192：24； AES256：32；
iv	是	用于存放初始化向量 IV 数据和返回的 IV 数据（不需要使用 IV 值的加密模式传一个任意非空字节数组即可）
ivLen	是	初始化向量 IV 数据字节长度，有效值如下： SM1、SM4、AES、AES192、AES256：16； DES、3DES：8

3.3.4 输出参数

OK，成功。其他，返回相应的错误码。

3.4 对称解密接口

3.4.1 接口说明

使用指定的密钥和IV,以及指定的对称密钥分组解密算法和工作方式对输入数据进行对称解密运算（对称解密接口需至少支持 1024×1024KB的数据大小）。

3.4.2 接口定义

public int symDecrypt (int alg, int mode, byte[] inData, int inLen, byte[] out, int[] oOutLen, byte[] keyData, int keyLen, byte[] iv, int ivLen);

3.4.3 输入参数

参数名称	是否必填	说明
alg	是	算法标识，有效取值如下： ALG_SM1：SM1 算法； ALG_SM4：SM4 算法； ALG_AES：AES 算法； ALG_AES192：AES192 算法； ALG_AES256：AES256 算法； ALG_DES：DES 算法； ALG_3DES：3DES 算法；
mode	是	对称运算工作模式，有效值如下： ALGMODE_ECB； ALGMODE_CBC； ALGMODE_CFB； ALGMODE_OFB； ALGMODE_CTR；
inData	是	用于存放输入密文数据
inLen	是	输入密文数据字节长度，有效值必须是算法分组长度的整数倍； SM1、SM4：16 的倍数； DES、3DES：8 的倍数； AES、AES192、AES256：16 的倍数；
out	是	用于输出解密明文数据
outLen	是	用于输出解密明文数据的字节长度
keyData	是	用于存放输入对称密钥数据。
keyLen	是	输入密钥数据字节长度，有效值如下： SM1、SM4、AES：16； DES：8；

		3DES：24； AES192：24； AES256：32；
iv	是	用于存放初始化向量 IV 数据和返回的 IV 数据（不需要使用 IV 值的加密模式传一个任意非空字节数组即可）
ivLen	是	初始化向量 IV 数据字节长度，有效值如下： SM1、SM4、AES、AES192、AES256：16； DES、3DES：8

3.4.4 输出参数

OK，成功。其他，返回相应的错误码

4. 数据常量定义

名称	常量值
ALGMODE_ECB	0x00000000
ALGMODE_CBC	0x00000001
ALGMODE_CFB	0x00000002
ALGMODE_OFB	0x00000003
ALGMODE_CTR	0x00000005
ALG_SM1	0x00000002
ALG_SM4	0x00000008
ALG_AES128	0x00000004
ALG_AES192	0x00000009
ALG_AES256	0x0000000A
ALG_3DES	0x00000003
ALG_DES	0x00000005

5. 错误码

接口返回码	说明
OK(0x000)	成功
ERR(0x001)	失败
UNKNOWN（0x003）	未知错误

NOTSUPPORT（0x003）	不支持
PARAERR（0x005）	参数错误
DEVICEBUSY（0x007）	密码设备繁忙
TIMEOUT（0x008）	超时
DATALENERR（0x015）	数据长度错误
KEYLENERR（0x016）	密钥长度错误
KEYNUMERR（0x017）	密钥号错误
DEVICLOSE（0x018）	密码设备关闭
CONNECTIONCOUNTERR（0x019）	连接数量错误
KEYNOTEXIST（0x0a0）	密钥不存在
IVLENERR（0x100）	Iv 长度不正确
ENCRYPTERR（0x185）	对称加密错误
DECRYPTERR（0x186）	对称解密错误