甲方合同编号：
乙方合同编号：

医院综合管理平台商用密码应用改造项目

销售合同

甲方(购买方)：西安医学院附属宝鸡医院

地址：陕西省宝鸡市渭滨区清姜路 4 号

法定代表人：焦晓虎 联系人： 王守刚 电话：09173212081 传真:

乙方（供货方）：北京海泰方圆科技股份有限公司

地址：北京市海淀区上地九街 9 号神州数码广场北区 6 层 611 号

法定代表人：姜海舟 联系人：曹坤 电话： 18729861715 传真： 010-62971615

客服： 010-58103330、 010-62968660

根据《中华人民共和国民法典》等相关法律法规的规定，甲乙双方经友好协商一致，于北京市海淀区签订本合同。

一、合同内容

本次采购合同将用于医院综合管理平台商用密码应用改造项目(招标编号:OTXA-2620021127)，用户为西安医学院附属宝鸡医院；甲方向乙方购买相关软硬件产品与服务，产品具体规格、性能、型号及相关要求见下表。

1. 产品明细表如下：

序号	产品名称	规格型号	品牌	数量	单价	总价
1	光电安辰国密高安全门禁系统	STC-1 V1.0	光电安辰	1 套	50000	50000
2	光电安辰安全音视频监控系统	SJT1708 V1.0	光电安辰	1 套	45000	45000
3	IPSec/SSL VPN 综合	HT-ISG V1.0	海泰方圆	2 台	35600	71200

	安全网关					
4	安全浏览器密码模块	SHM1602-G V5.0	海泰方圆	20 套	100	2000
5	管理运维人员 Ukey 智能密码钥匙及数字证书	智能密码钥匙 SJK1110-G	海泰方圆	20 套	100	2000
		数字证书(一年)	河北 CA			
6	密码服务管理平台	HT-CISP V3.0	海泰方圆	1 台	148000	148000
7	数据库加密机	HT-DCM V2.0	海泰方圆	1 台	40000	40000
8	服务器密码机	Haitai-ET V3.0	海泰方圆	1 台	45000	45000
9	服务器站点证书	服务器站点证书（一年）	河北 CA	1 套	3300	3300
总计		¥ 406500.00				

合同金额包括产品价款、包装、运保费、增值税、原厂商保修服务、技术支持及安装调试等供方履行本合同项下全部义务所需的一切费用，产品增值税率为 13%。

2. 服务地点：甲方指定地点

3. 服务期限：软硬件均为三年，数字证书、服务器站点证书为一年 。

二、合同组成

1.下述文件是构成本合同不可分割的部分:

（1）本合同条款及其所有附件。

（2）甲方的招标文件及澄清文件。

（3）乙方的投标文件及质疑解答文件。

（4）中标通知书。

（5）法定代表人授权书。

（6）双方与合同有关的往来信函、传真经双方法定代表人或其授权代表签字并加盖单位公章

确认后视为本合同的组成部分。

（7）经双方法定代表人或其授权代表签字并加盖单位公章确认的补充协议。

2.如果乙方的投标文件及质疑解答文件内容违背或低于甲方招标文件要求或任何可能导致影响当次采购目的的情形，均应当被视为乙方自动放弃投标文件及质疑解答文件中相应部分而同意以招标文件相应内容为准。如果乙方的投标文件及质疑解答文件内容高于甲方招标文件要求，则以乙方的投标文件及质疑解答文件内容为准。如果合同条款与合同附件有矛盾之处，以合同条款内容为准。如果合同附件之间有矛盾之处，以有利于甲方的附件内容为准。

3.上述合同文件应能够相互解释、相互说明。如合同文件之间出现不一致，除本合同另有约定外，第（1）款至（6）款的排列顺序就是合同文件的优先解释顺序。对于第（7）款中双方达成的补充协议与原合同（包括（1）-（6）款中所列的所有文件）存在不一致，以签订日期在后的补充协议为准。

三、 合同价款及支付方式

1. 合同总价款为 RMB ¥406500.00 元(大写： 人民币肆拾万陆仟伍佰元整)，

2. 合同签订，安装调试验收合格 3 个月后 ，达到付款条件起 30 日内， 支付合同总金额的 30.00%，计：¥121950.00 元(大写：人民币壹拾贰万壹仟玖佰伍拾元整)；合同签订，安装调试验收合格 6 个月内 ，达到付款条件起 30 日内， 支付合同总金额的 60.00%，计：¥243900.00 元(大写：贰拾肆万叁仟玖佰元整)，合同签订，安装调试验收合格 24 个月后 ，达到付款条件起 30 日内， 支付合同总金额的 10.00%，计：¥40650.00 元(大写：肆万零陆佰伍拾元整)。

3. 乙方账户信息：

◆ 开户银行：工行海淀支行营业部

户 名：北京海泰方圆科技股份有限公司

账 号：0200049609200087597

4. 乙方账户信息如有变更，应于约定的付款日提前五个工作日以书面形式通知甲方。

四、交货验收及发票

1. 实施时间：乙方于合同生效后 1 月后实施。

2. 乙方按照甲方要求确保产品安全无损到达交货地点。在产品交付以前产生的运输费、保险费由乙方承担。

3. 交货地点：甲方指定地点

联系人： 王守刚 联系电话：09173212081

4. 乙方安装、调试完毕，配合医院完成商用密码测评工作，测评达标，正常运行 30 天后方可

向甲方提出书面验收申请。

甲方开票信息：

发票类型： 普通发票

开户名称：西安医学院附属宝鸡医院 地 址:陕西省宝鸡市渭滨区清姜路 4 号

开户行:长安银行宝鸡高新支行 账 号：806021401421002757

五、甲乙双方责任

甲方责任：

1. 甲方承认本项目涉及的软硬件有关的源代码、文档资料的知识产权全部归乙方所有。

2. 甲方不得将本项目向第三方提供、销售、出租、出借、转让或提供分许可、转许可，通过信息网络传播或以其他形式供他人利用。

3. 甲方不得对本项目涉及的软硬件进行全部或部分地翻译、分解、反向编译、反汇编、反向工程或其他试图从本项目软件中导出源代码的行为，或在本项目软件的基础上书写或开发衍生软件、衍生产品或其他软件。

4. 甲方需配合乙方提供安装、实施、部署所需的场地；安装软件所涉及的软硬件环境等各类条件。

5. 甲方需按付款方式按期向乙方支付合同款项。

乙方责任：

1. 乙方依法对项目软硬件拥有知识产权、处分权、使用权、所有权。

2. 乙方应保证本项目的实施、部署与验收工作，保证按期、按质完成项目验收。

3. 乙方负责本项目的运维服务工作，服务期限自验收之日起 天。

4. 为保证系统正常、安全地运行，乙方应据此提供技术支持服务，及时解决故障，30 分内响应，4 小时内到达现场。系统运行正常前，必须有专人驻场运维。

5. 乙方须为甲方提供本项目的产品使用、操作和管理维护培训，培训形式可采用客户现场培训、或远程课堂培训。

五、售后服务

1. 本项目所投上述产品，软硬件均提供三年免费质保服务，招标文件中要求的站点证书为一年的除外。

2. 作为本次项目货物的原厂商，售后服务提供原厂备件、技术支持、维修服务等，保障项目顺利推进。

六、技术培训

1．产品交付或项目验收后乙方需根据甲方需要提供相应的技术材料。

2．若甲方需要乙方提供现场技术培训，应当提前十五日通知乙方，以便乙方做好培训准备。

七、知识产权

1．本合同所载软件产品的知识产权归乙方所有，未经乙方书面许可，甲方不得对此软件进行修改，不得以乙方的软件为基础进行其他开发，不得将本软件产品出售、拷贝、复制或泄露给第三方使用，否则应承担相应的法律责任。

2．乙方认同甲方拥有本合同所载软件产品的不可转让的非独占的使用权。

八、免责条款

1．乙方对于甲方因使用本软件而造成的任何间接的、附带的或随之而起的损失，如商业机会的丧失、利润的减少等均不承担责任。

2．乙方对甲方因自身原因导致本软件遗失、被盗、被误用或擅自修改、计算机设备故障、操作失误等情况造成的损失不负任何责任。

九、保密协议

1．在合作过程中，任何一方对从对方获取的商业秘密、信息严格保密，在未事先取得另一方书面同意的情况下，不得向任何第三方披露，同时保证因为工作需要接触商业秘密、信息的该方员工严格保密，否则应承担对方因此而受到的损失，且该保密义务不因本协议的终止而终止。但该信息符合以下任何一项或多项情形的除外：（1）披露方以书面方式明确注明为非保密性质的信息；（2）公众已经知晓的或通过公开渠道可获得的信息，且不是因为接受方违反本保密义务而导致该信息被公众知晓的；（3）接受方从有权披露该信息的第三方获取的信息，且接受方对该信息无保密义务；（4）在本合同谈判前接受方已独立开发的信息；（5）按法律需求向任何机关、机构、媒介公开的内容。

2．保密信息是指任何一方依照本协议向对方所披露的所有非公开的专有信息或资料。包括但不限于任何一方的产品信息、软件程序、商业运作、技术、业务活动、资金状况、客户资源、财务有关的任何非公开信息。

3．除本协议规定之工作所需外，未经对方事先同意，不得擅自使用、复制对方的商标、标志、商业信息、技术及其他资料。

十、承诺与保证

1．双方清楚地知悉对方的经营范围、授权权限。双方都已阅读本合同所有条款，并对本合同条款的含义及相应的法律后果已全部知晓并充分理解。

2．双方保证都具备签署本合同的合法资格，并且在本合同项下的行为符合法律、行政法规、规章规定，双方签署本合同或履行在本合同项下的义务不违反各自订立的任何其他协议，双方在本合同项下的行为符合各自的章程或内部组织文件的规定，且已获得必要的公司（机构、组织）内部

有权机构及/或国家有权机关的批准。

3．双方保证提供给对方的全部资料、文件和信息均是真实、合法、准确、完整、有效的。

十一、违约责任

1．甲方违约处理：

(1)甲方不按照本合同规定支付款项，经乙方催告后 五个工作日内仍未支付的，从催告期间届满之日起，每日向乙方偿付未支付合同价款的千分之五的违约金。此项违约金额以逾期付款部分总值的百分之十为限。

(2)甲方违反“知识产权”、“保密协议”、“承诺与保证”条款中任一约定的，应按合同价款总额的百分之十向乙方支付违约金。违约金不足以弥补乙方损失的，甲方还应赔偿乙方因此遭受的全部损失。

(3)甲方应当向乙方支付违约金或赔偿金的，应当在乙方发出索赔通知后十五日之内支付给乙方。

(4)甲方有其他违约行为给乙方造成损失的，应对造成的损失进行赔偿。

2．乙方违约处理：

（1）乙方不按照本合同的规定准时交货，经甲方催告后五个工作日内仍未交货的，每日向甲方支付未交付货物合同总额的千分之五的违约金，此项违约金额以逾期交货部分货物总额的百分之十为限。

（2）乙方应当向甲方支付违约金或赔偿金的，应当在甲方发出索赔通知后十五日之内支付给乙方。

(3)乙方有其他违约行为给甲方造成损失的，应对造成的损失进行赔偿。

3．其他违约：

任何一方无故解除合同或其他不符合合同规定的行为均视为违约，应承担但不限于因其行为给对方所造成的损失的赔偿。

4．本条所称损失的范围包含但不限于直接损失和守约方在合同正常履行后的可得利益、实现债权的费用（含律师代理费、差旅费等）。

十二、不可抗力

1．“不可抗力”是指甲乙双方无法控制、无法预见且无法避免的事件，该事件妨碍、影响或延误任何一方根据协议履行其全部或部分义务。该事件包括但不限于政府行为、重大自然灾害、大规模战争等；电信部门技术调整、黑客攻击、网站遭到破坏、瘫痪或无法正常使用及非因甲方过错导致的甲方机房故障、服务器故障或不能正常运行等。

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书面详情及将有关证

明文件送交对方。

3．发生不可抗力事件时，甲乙双方应协商以寻找一个合理的解决方法，并尽一切努力减轻不可抗力产生的后果。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。

十三、争议解决

1．因本合同引起的或与本合同有关的任何争议，双方应通过友好协商的方式解决，协商不成的向合同签订地人民法院起诉。

2．本合同之签署、生效、解释和执行以及本合同项下争议之解决，均应适用中华人民共和国法律（不含港澳台地区）。

十四、其他事项

1．任何一方提出的对本合同的补充或修改，应由双方协商一致以书面文件形式确定。本合同的附件作为合同的有效组成部分和本合同具有同等的法律效力。

2．如果本合同的任何条款被司法机关或其它有权机关宣布为无效、非法或其它形式的不可执行，本合同其它条款仍然有效，双方均应遵照执行。

3．本合同经双方签字盖章后生效，如双方签字盖章日期不一致的，以最后签字盖章日为合同生效日。本合同一式肆份，双方各执贰份，具有同等法律效力。

（以下无正文）

甲方： 西安医学院附属宝鸡医院

（公章）或（合同章）

授权代表（签字）：

2026 年 7 月 9 日

乙方：北京海泰方圆科技股份有限公司

（公章）或（合同章）

授权代表（签字）：

2026 年 7 月 9 日

附件一：产品规格、性能、技术标准及相关要求

服务内容	产品名称/型号	描述	单价	单位	数量	金额（元）	交货形式
国密门禁系统	光电安辰国密高安全门禁系统/STC-1 V1.0	1.国密门禁系统1套：内置国产安全芯片，防水等级≥IP54，国产安全算法，具有抓拍预警功能。支持人脸识别加刷卡双认证开门方式；人脸比对速度 白天≤300ms 夜间≤500ms；人脸特征值存储容量≥5000条;CPU卡存储容量≥5000条；国密门禁系统具备商用密码检测中心颁发的商用密码产品认证证书。 2.门禁系统采用的安全芯片具备商用密码检测中心颁发的商用密码产品认证证书 。 3.门禁系统采用的门禁卡≥20张（智能IC卡），具备商用密码检测中心颁发的商用密码产品认证证书。 4.门禁控制器1台:内置国家密码局认证的安全芯片，采用国密算法与门禁机前端进行加密通讯； 5.后台登录读卡器1台:通过管理员密码及国密卡硬件介质双重认证对后台登录人员进行身份认证;含≥5张用户登录国密卡。 6.门禁配件：开门按钮，磁力锁、磁力锁支架等1套； 7.门禁管理系统配套硬件1	50000	套	1	50000	实物

		套:CPU:≥四核，≥2.0GHz，硬盘:≥256GSSD+1T 机械硬盘;内存:≥8G；国产操作系统；安装门禁管理后台软件，实现门禁设备管理;后台系统与门禁前端通讯采用加密技术。					
国密视频监控	光电安辰安全音视频监控系统/SJT1708 V1.0	1.国密视频监控 1 套，需符合 GB35114-2017 公共安全视频监控安全技术要求，符合国密标准，满足密码测评要求，支持≥16 路前端接入，支持 SVAC2.0、H.264、H.265 等编码，接入≥64Mbps，储存≥64Mbps，转发≥32Mbps，≥8 路录像回放（单路 4Mbps 1080P）WEB 单客户端支持≥4 路 1080P 4M 码流解码。WEB 客户端支持验签及解密播放。显示输出接口：≥1 个 VGA，≥2 个 HDMI，≥2 个千兆网口；含监控硬盘，存储监控数据≥180 天；2.国密网络摄像机 3 台：图像传感器:≥1/2.7”CMOS;镜头焦距:f=2.8-12mm;≥400 万像素;支持支持人脸检测抓拍、通用行为分析算法切换，走廊模式;红外夜视距离≥10 米;视频编码标准:支持 SVAC2.0/H.265。≥256GB 存储卡本地存储扩展，报警≥1 入 1 出；内置通过商用密码检测认证中心检测认证的安全芯片，支持	45000	套	1	45000	实物

		SM1/SM2/SM3/SM4 等国家商用密码算法。 3. 提供商用密码检测认证中心颁发的《商用密码产品认证证书》。					
认证加密传输综合安全网关	IPSec/SSL VPN 综合安全网关 /HT-ISG V1.0	1. 产品规格：标准机架式设备，国产操作系统、国产 CPU, 千兆电口≥6 个，千兆光口≥4 个，冗余电源； 2. 性能要求：SSL 加密带宽≥900Mbps、最大用并发用户数 ≥3000 个、最大用户数≥10000 个；IPSec 加密带宽≥900 Mbps；并发隧道数≥1000； 3. 提供国密标准 IPSec 加密，SSL 加密，以及数字证书认证与管理等认证网关功能。 4. 支持国密 SM1/SM2/SM3/SM4 算法。 支持反向代理、SSL VPN 隧道、IPSec VPN 隧道工作模式。 5. 支持“多对一”地址转换，使得内部网络主机访问外部网络时，其源 IP 地址被转换；支持“一对多”地址转换，将内网服务器的 IP 地址/端口映射外网接口的 IP 地址/端口，使外部网络的主机通过访问映射地址和端口实现对内部服务器的访问。 6. 支持 SNAT 模式，代理内网原地址转换模式，或普通路由模式。	35600	台	2	71200	实物

		7.支持基于用户名、群组、角色；基于用户数字证书信息；基于目标应用系统；基于CRL证书吊销列表的访问控制。 8.支持标准SSL安全协议、IPSec安全协议，支持国密算法及国际算法，数据传输过程中实现数据加密传输。 支持国密算法套件。支持SSL3.0、TLS V1.0/V1.1/V1.2/V1.3，同时支持国密标准SSL协议GMTLS V1.1。 9.支持智能终端、应用APP、PC、手机等设备接入，支持用户终端安全检查。 10.支持用户、用户组管理，提供细粒度控制，到同应用的权限划分。通过给不同用户设置不同角色来分配访问授权，一个用户可以赋予多个角色以适合各种复杂的组织结构。 11.支持用户名分别与终端硬件特征码绑定。。 12.支持基于用户/用户组的连接数控制。 13.支持联动CA系统,通过离线CRL导入，在线CRL、SCEP协议等方式实时验证用户状态。。 14.支持客户端零痕迹访问、缓存清空、Cookie清空、访问记录清空、					

		硬件特征码绑定，支持客户端互联隔离功能，接入后无法访问隧道外资源。 15.客户端 APP 支持 windows、linux、Android、IOS、国产等多种操作系统。 16.具备商用密码检测认证中心颁发的《商用密码产品认证证书》第二级及以上，产品符合 GM/T0023《IPsec VPN 网关产品规范》、GM/T0025《SSL VPN 网关产品规范》和 GM/T0028《密码模块安全技术要求》第二级要求。					
国密浏览器	安全浏览器密码模块/SHM1602-G V5.0	1.具备商用密码检测认证中心颁发的《商用密码产品认证证书》第二级及以上； 2.支持 SM2、SM3、SM4 等算法，保证 Web 网页访问的安全性。 3.支持兼容主流国产操作系统和主流国产 CPU 环境。	100	套	20	2000	光盘
管理运维人员 Ukey 智能密码钥匙及数字证书	智能密码钥匙/SJK1110-G	1.具备商用密码检测认证中心颁发的《商用密码产品认证证书》第二级及以上； 2.符合 USB2.0 规范，兼容 USB1.1，兼容 3.0 规范接口； 3.支持国密算法 SM2、SM3、SM4，	100	套	20	2000	实物
	数字证书						电子邮件

		支持 CSP/PKCS#11/SKF 开发接口； 4. 支持存储数字证书，支持 X.509 v3 标准证书格式。 5. 包含国家认可的第三方个人数字证书，1 年授权。					
统一密码服务平台	密码服务管理平台/HT-CISP V3.0	1. 产品规格：标准机架式设备，国产操作系统、国产 CPU,千兆电口≥4 个，冗余电源； 2. 应用系统接入数≥50 个，设备接入数≥40 个，支持用户数≥1000，密钥生成速度≥15000 次/秒。 3. 产品支持国密和国际通用算法： （1）对称算法：SM4 （2）非对称算法：SM2 （3）摘要算法：SM3 4. 支持对密钥全生命周期管理，包括密钥生成、存储、分发、导入与导出、密钥使用、密钥更新、密钥备份与恢复、密钥归档、密钥吊销、密钥销毁等管理服务； 5. 支持对密钥模板、密钥生成、密钥分发等能力进行策略管理； 6. 兼容对接及适配多厂商密码设备，支持但不限于服务器密码机、签名验签服务器、加密安全网关等； 7. 支持应用系统的凭据的安全管理、对凭据密钥的全生命周期管理，支持多凭据管理； 8. 支持对密码资源进行资源注册、	148000	台	1	148000	实物

		资源分组、资源组分配管理，同类密码设备可按类型进行分组管理，分组后的设备可按照组内设备策略统一对外提供服务，实现密码资源的精细化管理。 9.支持平台监控大屏展示，可对平台密码设备、密码资源以及密钥的使用情况展示，让用户对系统内资源使用情况一目了然。 10.支持多种调用方式：提供支持主流国产操作系统等的多种调用接口，提供标准 API 等接口，支持 Restful 接口调用方式，接口至少支持 C/C++、Java 接口。 11.提供密码服务插件与业务软件整合，屏蔽密码设备服务接口开发的复杂性，实现对业务系统提供各种密码计算及密码服务的能力，对各种密码运算、密码服务、密码管理等接口进行封装处理，提供简单易用的安全开发接口，业务系统软件开发人员无需关心底层密码运算的具体实现，降低集成工作的复杂度和开发成本； 12.支持密码资源智能调度，保障业务系统自动过滤故障的密码资源，保障业务系统对密码运算服务的良好使用； 13.灵活对接调用各种密码设备和					

		服务，达成整个系统的密码改造合规； 14.产品软硬一体化部署，内置具有商用密码检测认证中心颁发的商用密码产品认证证书的安全二级密码卡； 15.产品为完全自主研发获取，拥有完全自主的知识产权，具有计算机软件著作权登记证书； 16.必须同时具备商用密码检测认证中心颁发的密码服务管理平台以及密钥管理系统《商用密码产品认证证书》第二级及以上。					
存储加密服务器	数据库加密机/HT-DCM V2.0	1.服务器：标准机架式≥2U、 2.国产 CPU≥1 颗、CPU 核数≥64 核，主频≥2.0GHz 内存：≥64G； 3.网络：≥2 个万兆光接口(配万兆模块)，≥2 个千兆电口； 4.电源：双冗余电源； 5.系统盘：SSD，≥128G； 6.数据盘：支持≥8 块，本次配置≥32T。 7.操作系统：支持国产操作系统。 8.实现数据库系统的实时安全加密，支持国产数据库。 9.产品可应用于结构化、半结构化和非结构化等复杂结构数据的加密存储。 10.支持 SM1，SM2，SM3，SM4 等国	40000	台	1	40000	实物

		密算法； 11.提供商用密码检测认证中心颁发的《商用密码产品认证证书》第二级及以上。					
服务器密码机	服务器密码机/Haitai-ET V3.0	1.标准机架式设备，内置硬盘≥240GB SSD，千兆电口≥4个；万兆光口≥2个（配万兆模块），双冗余电源； 2.性能要求：SM1加解密≥5Gbps，SM2签名≥80000次/秒，SM2验签≥30000次/秒，SM3杂凑≥6Gbps，SM4加解密≥6Gbps。 支持SM1、SM4算法的数据加密、解密服务。 3.支持SM2算法的签名和验签。 4.支持SM3算法的数据摘要计算功能 5.支持基于SM2算法的密钥协商功能。 6.支持SM1、SM4及SM3等算法的消息认证码计算功能。 7.支持≥10万条密钥的管理能力。 8.支持对应用系统进行IP白名单访问控制，白名单支持IP地址或IP段两种访问控制策略，可根据管理要求，配置IP白名单的生效时间。 9.支持日志等级设置，可设置为DEBUG、INFO、WARN、ERROR等多个	45000	台	1	45000	实物

		等级，且支持通过数字签名的方式实现日志数据完整性保护。 10.支持将设备内的密钥等重要信息加密后采用门限方式进行备份。 11.支持对接密钥管理系统、密码服务平台等； 12.支持与符合《GM/T 0050-2016 密码设备管理 设备管理技术规范》的密码设备管理平台对接； 13.支持多种高可用能力，支持第三方负载均衡器，支持自负载； 14.提供商用密码检测认证中心颁发的《商用密码产品认证证书》第二级及以上； 15.内置国密局核准的安全二级密码卡，内置密码卡与服务器密码机必须为同一品牌，密码卡及服务器密码机均具有商用密码检测认证中心颁发的《商用密码产品认证证书》第二级及以上，并符合 GM/T0028《密码模块安全技术要求》第二级要求。					
服务器站点证书	服务器站点证书	双算法自适应 SSL 证书，为服务器站点提供身份鉴定并保证该网站拥有高强度加密安全，保证网站的真实性，有效性，防止钓鱼网站。连续 1 年服务授权。	3300	套	1	3300	电子邮件