GoUpSec
升华安全佳

2022 中国网络安全行业

商用密码产品及服务购买决策参考

2022 年 11 月发布版

目录

前言

网络安全的“新基建”：商用密码

商用密码是网络安全的基石，也是中美网络空间“新基建”竞争的重要战略资源。

今年 10 月份，拜登政府发布美国国家安全备忘录并明确指出：将不懈关注国家关键基础设施防御的改善，建立一个全面的方法来**“锁紧美国的数字大门”**，并强调将通过开发新的加密技术来“建立美国技术优势，保护未来的在线商务和国家机密。”

11 月，特斯拉创始人马斯克入主 Twitter 的第一件事不是急于开发“类似微信的新功能”，而是开除了 Twitter 整个网络安全团队，并宣称将为 Twitter 私人消息开发端到端加密功能。

密码技术是维护网络安全最有效、最可靠、最经济的技术手段。2022 年从关键基础设施到消费互联网，越来越多的政府机构和企业开始主动使用密码技术强化数据安全和个人信息保护，重构网络信任体系。

今天，密码技术已经成为下一代互联网的“底层逻辑”，“密码霸权”阴影下数字经济的“定海神针”，更是 “关键基础设施安全”和“关键核心技术安全可控”的核心要素。

商用密码迎来“最好的时代”

近年来随着数字化转型、云计算、物联网、5G、大数据等数字化进程加速，疫情推动的远程办公和混合办公导致攻击面不断扩大，数据加密脱敏，漏洞管理、

访问控制等环节的风险不断增长，全球关键基础设施多次发生大规模数据泄露事件，已经为各国政府敲响警钟。

白宫的国家安全战略强调密码技术普及和创新的重要性，希望通过（抗量子加密等）商用密码技术创新巩固美国的“密码霸权”。

我国作为全球第二大经济体，密码配套政策法规和标准化工作近年来也紧锣密鼓开展，2020 年 1 月《密码法》的颁布实施；2021 年 10 月 1 日，国家密码应用与安全性评估的关键标准(GB/T 39786)正式实施，明确指出等保三级要求所使用的密码产品应达到二级及以上安全标准。

在“密评密改”等合规性需求刺激下，中国的商用密码市场进入了高速增长期，根据华经产业研究院报告，2020 年在新冠疫情流行的客观环境下，我国商用密码产业仍取得高速发展，总体规模达到 466 亿元，较 2019 年增长 33.14%，预计 2023 年商用密码行业规模有望达到 937.5 亿元。

在关键基础设施领域，随着我国《关键基础设施安全保护条例》（2021 年 9 月）的实施，以及首个关键基础设施国家标准《信息安全技术 关键信息基础设施安全保护要求》（2023 年 5 月 1 日实施）的颁布，将进一步推动商用密码应用市场的发展。

《标准》提出了关键信息基础设施安全保护 3 项基本原则：

- 以关键业务为核心的整体防控
- 以风险管理为导向的动态防护
- 以信息共享为基础的协同联防

无论是“整体防控”、“动态防护”还是“信息共享”，都对关键基础设施的网络安全和数据加密提出了更高的要求。

此外，关键基础设施国家标准还明确强化检测评估（至少每年一次），推动等保制度落实、商用密码应用、供应链防护、数据安全的安全性评估。过去，我国地方政府政务服务平台的数据加密及密码应用环节薄弱，使用非国产密码算法的现象也比较普遍。在法规和标准化的“双管”推动下，商用密码应用正从省部级平台逐步向市区级平台纵向和行业横向延伸，区域密码工作正蓬勃开展。

与此同时，我国商用密码产品自主创新能力持续增强，产业支撑能力不断提升，商密标准体系逐步完善，密码国产化和密码改造与其他网络安全产品和生态的整合加速，商用密码产业将迎来长期且持续的发展机遇。

商用密码的选型

随着云计算、大数据、物联网、车联网、区块链、数字货币、远程办公等商用密码新场景和新需求的涌现，商用密码市场蓬勃发展，密码应用安全建设已经成为我国网络安全建设的第三大合规市场。除了传统密码厂商，还有许多科技和安全企业也已经或正在进入这个赛道，并陆续推出自己的密码卡、服务器密码机、安全认证网关等密码类产品。

目前，我国商用密码市场百花齐放，现有商用密码产品达到 3000 余款，其中 2200 余款产品取得商用密码产品认证证书，部分产品性能指标已达到国际先进水平。品类涵盖了密码芯片、密码板卡、密码整机、密码系统等全产业链条，形

成了完整的商用密码产品体系和算法体系，产品主要分为以下六类：

- 密码算法类：提供密码运算功能，加密卡、密码芯片等。
- 数据加解密：提供数据加解密功能产品，如服务器密码机、云服务器密码机、VPN 加密网关和加密硬盘等。
- 认证鉴别类：提供身份鉴别等功能产品，如认证网关、动态口令、令牌环，签名验证服务器。
- 证书管理类：提供证书产生、分发、管理功能的产品，如证书认证系统等。
- 密钥管理类：提供密钥产生、分发、更新、归档和恢复等功能的产品，例如证书认证密钥管理系统、支付服务密钥管理系统等。
- 密码防伪类：提供密码防伪验证功能的产品，例如电子签章、时间戳服务器。

由于商用密码行业较为分散，尚未形成产业集群优势。未来五年，商用密码应用市场将呈现网络安全企业与传统密码厂商之间相互竞争又相互融合的新局面。

商用密码应用面临的挑战

- **合规驱动。**商用密码市场目前仍然是合规驱动为主，等保和关基用户关注的重点是旧密码系统的改造、升级与合规。新场景需求尚未得到充分释放和有效监管。
- **选型困难。**商用密码市场分散、应用体系复杂、产品种类繁多，企业难以对商密产品体系的合规性、安全性以及“自主可控”等进行全面评估。

- **整合困难。**密码应用和升级改造涉及算法、协议、产品、技术体系、密钥管理、密码应用等多个方面，统一密管、统一认证、数据加密、云安全和移动安全的密码应用运营管理体系的建设还面临与其他安全产品方案(例如零信任) 和信息系统的整合和统一管理问题。

- **人才短缺。**与其他安全领域技术升级面临的困境类似，企业用户普遍缺少专业密码技术人才，密码应用的需求、规划和实施能力较弱。

产品与服务的选型参考基准：

针对企业商业密码/国产密码应用面临的挑战，商业密码产品和方案选型除了需要安全合规 (例如密码产品资质以及密评工作指导文件《信息系统密码应用高风险判定指引》等)，还可参考以下选型基准建议：

- **可管理性和可见性。**包括密评密改工作进度和成果的可视化监控和管理。

- **自主可控。**采用国密算法进行数据传输和存储加密。

- **云原生架构。**密码管理和服务平台的云原生开发部署和管理、可量化、统一资源一站式管理、弹性扩容、云安全。

- **系统化建设。**统一建设密码服务平台，确保为应用系统提供统一、标准、规范、便利、安全、可扩展、易维护的密码服务，同时能够满足建设单位对应用系统密码应用的安全需求以及管理要求。（SSO 应该是“标配”产品，不是奢侈品。）

- **产品自身的安全性，减少密码应用系统带来的新的攻击面。**

- **与其他安全产品和方案的可集成性和可扩展性。**

- **厂商的专业服务与持续开发能力。**
- **身份认证采用高强度 MFA 多因素认证（基于 PKI、硬件密钥或 APP）。**遏制和缓解中间人攻击以及社会工程攻击威胁。

GoUpSec 深入调研了多家知名国内商用密码专业提供商和综合安全厂商，从产品功能、应用行业、成功案例、安全策略等维度对各厂商商用密码产品及服务进行调研了解，整理形成了 2022 年中国网络安全行业《商用密码产品及服务购买决策参考》。

本次报告共收录 16 家国内网络安全厂商，共计 37 个商用密码产品及服务，成功实施案例 44 例，分别来自政府、金融、运营商、能源、医疗、物联网、车联网、电力、交通、公安、制造业、医疗、互联网、地产、教育等重点行业。

**由于市场调研工作或时间局限等原因，部分商用密码厂商暂未报名参与此次调研，后续我们将继续补充完善相关名录。*

安盟信息

一、公司名称：

北京安盟信息技术股份有限公司

二、公司 logo：

三、商用密码产品名称：

安盟华御密码应用监测平台

安盟华御密码服务平台

四、产品特点及优势：

安盟华御密码应用监测平台：

特点：

契合密码主管部门的管理模式，支撑主管部门行使监督检查指导等职责

推进密评工作推进的环节把控，实现密评密改工作状态一窗式管理呈现

支撑全局视角下的密评可视化，实时获取信息系统的密码应用运行情况

分区域分行业展示密码工作成果，全局化呈现密码工作推进成效与趋势

优势：

依据主管部门的管理逻辑，提供更贴身的密码工作管理工具

细化密评密改项目逻辑，从参与角色出发

支持级联部署，实现省市县多级密码应用工作统筹

多维度多角度梳理区域密码工作进展，综合化展现发展趋势和建设成效

安盟华御密码服务平台：

特点：

通过平台化集约化设计，统一资源管理，统一服务接口

提供标准化组件化服务能力，支持用户应用快速对接、快速上线

云原生架构设计研发，支持容器化部署和多租户隔离

支持对密码应用情况进行健康度监测

优势：

支持云原生部署运维，管理简便，支持快捷、自动化扩容；

支持对应用的认证授权和细粒度访问控制；

支持基于流量、应用、时间等要素的配额管理和流量控制；

提供密码事件库、规则库对密码应用的态势进行风险预警和报警。

五、成功案例：

安盟华御密码应用监测平台：

为某市密码主管部门部署密码应用监测平台，提供区域级密码应用情况的监测和展示，为主管部门提供密评密改统一管理、密码应用环节把控、密码应用态势呈现、信息采集逐级汇聚等能力，聚合了主管部门、业务单位、产品厂商和测评机构，为当地密码工作的开展提供了有效的工具支持。

安盟华御密码服务平台：

为某市政务云部署密码服务平台，提供平台化可运营的密码服务能力。在政务云上发布密码服务，某委办局的信息系统通过采购云上的密码服务获取满足密评要求的密码保障能力。

六、适用行业：

密码及行业主管部门、政务云平台、央企云平台、行业云平台

七、联系人姓名及职位

姓名：张莉

职位：市场

联系方式：13701191423

八、**CEO/创始人/总裁/副总裁/联合创始人等对行业发展和甲方的寄语：**

三分技术，七分管理。随着密码应用从省部级平台逐步向市区级平台纵向和行业横向延伸，区域密码工作蓬勃发展，如何有效的统筹与督导区域工作、检查和指导各业务单位的密评工作开展情况成为密码主管部门的一个重要任务。

密码应用监测平台能够协助密码主管部门行使密码应用监督检查指导等职责、开展区域内商用密码事中事后监管、支撑区域内商用密码工作监督管理、完善区域内密码应用信息采集机制展现区域内商用密码应用整体态势、构建区域内密码应用动态监测能力，成为密码主管部门开展密码工作如臂使指般的工具和平台。

随着各省市政务部门、行业企业纷纷开展上云上平台，密码应用建设的主体环境也随之迁移到云平台上，密码服务平台基于其云原生、租户隔离、集约赋能、一站管理、可计量可管控、可监管可预警等特性，能够为政务云、行业云、企业云运营机构和业务单位提供按需调用、弹性扩容、易用好用的密码服务，为运维人员提供分权分域、一窗统管的运维管理能力，为运营商提供全网覆盖、一键直达、多维可视、一图概览的密码应用态势，成为云运营单位对外发布、管理和运营密码服务的核心基础承载平台。

——北京安盟信息技术股份有限公司商用密码发展中心总经理 韩斐

奥联

一、公司名称：

深圳奥联信息安全技术有限公司

二、公司 logo：

三、商用密码产品名称：

1.统一密码服务平台

2.数据库加密系统

四、产品特点及优势：

特点：

统一密码服务平台：

在国家信息化建设的不断推进以及网络安全已上升为国家战略的大背景下 ,奥联

统一密码服务平台整合了各厂家的密码资源，直接面向业务应用场景，提供统一的密码资源池管理、统一的系统运维监控、统一的密码接口规范、统一的密码策略配置、统一的密码安全应用管理，从而实现统一用户管理、统一身份认证、统一密码应用、统一运维监控的效果，满足应用信息系统的安全合规要求、密码技术的统一标准化改造和密码资源的统一管理与运维等要求。政府及企事业单位无需另行建设密钥基础设施，即可实现为各单位密码应用场景提供标准化的密码服务。

数据库加密系统：

数据库加密系统是奥联一款为保护数据、增强数据库系统的安全性，满足数字资产等级化的安全防护要求而自主开发的系统。该系统可通过字段级别的加密来达到对敏感数据的防护目的，应用时不需要改动基于数据库的应用系统，且不明显降低数据库的性能。

数据库加密系统能有效的帮助各信息系统进行改造，使其符合商用密码管理政策和《GB/T39786-2021 信息系统密码应用基本要求》、《信息系统密码测评要求》等相关密码标准规范，满足等保、关保、密评等对数据的机密性和完整性保护的要求。

优势：

统一密码服务平台：

1.多样的密码资源管理

统一密码服务平台提供统一的密码资源资源池管理功能，可实现对不同厂家密码机、加密服务器、签名服务器等密码基础设施的统一集中管理，对不同时期建设的密码设备进行统一管理和调度，降低运维人力物力，提高资源利用率和系统性能。

2.多密码体制融合技术

统一密码服务平台融合了 IBC 标识密码体制、PKI/CA 数字证书体制、无证书公钥密码体制构建整合的密码基础设施，支持 SM2/SM3/SM4/SM9 等国密算法，也支持 RSA/AES/3DES/SHA256/SHA512 等国际算法，可实现标准化、开放化的灵活部署，适合各种业务场景和设备能力。

3.适配国产环境

统一密码服务平台获得国家商用密码产品认证证书，支持鲲鹏、兆芯、飞腾等国产服务器和银河麒麟、中标麒麟、统信等国产操作系统。

数据库加密系统：

1.高安全性

数据库加解密系统获得了国家商用密码产品认证证书。数据库系统使用该产品后，敏感数据以密文的形式存在，即使是物理存储介质丢失或者数据库文件被非法复制的情况下，也能保证数据安全，杜绝泄露风险。

2.全场景适配

数据库加解密系统可提供 JDBC 插件、加密代理以及加密 SDK 等多种产品形态；支持透明拦截所有 SQL 语句，不改变应用系统原有的运行机制，应用免改造；不改变用户使用方式，用户无感知。

3.采用灵活的策略配置

数据库加解密系统支持对库表列的详细策略设置，包括元数据的定义、密钥策略定义，脱敏策略定义、哈希策略定义，并可以与第三方策略管理平台对接实现灵活的加密策略、完整性保护策略和动态脱敏策略。

4.支持多种数据库

数据库加解密系统支持各种主流关系型数据库，包括 oracle、DB2、MySQL、SQL server、PostgreSQL 等；支持国产数据库，包括人大金仓、达梦等数据库；支持非结构化数据库，包括 MongoDB 等。

五、成功案例：

XX 省统一密码服务平台-某数据中心客户项目

业务场景：

XXX 省互联网上承载的应用系统众多，各系统的安全及密码应用环节比较薄弱，存在普遍性安全隐患。目前，在身份识别、安全隔离、信息加密、完整性保护、抗抵赖性上存在系统性缺失 ,在部分应用密码的环节领域使用非国产密码算法的

现象也比较普遍。

客户需求：

- 用户鉴权信息的保护 :目前 XX 省云密码服务的身份认证采用口令方式认证，口令在传输过程中可能被截获或服务器可能被撞库攻击，需采用基于国密的身份认证技术进行改造。
- 敏感数据的保护：在用户浏览器侧/移动终端至应用边界服务器之间数据传输需采用密码技术保证重要数据在传输、存储过程中的机密性和完整性，包括但不限于鉴别数据、重要业务数据和重要用户信息等。
- 传输通道的保护：各单位上传或调用 XX 省云密码服务中的数据时，传输通道需要采用 VPN 通道加密方式对通道中传输的数据进行保护。

解决方案：

- 建设统一密码服务平台，部署于省级政务云上，确保为应用系统提供统一、标准、规范、便利、安全、可扩展、易维护的密码服务，同时能够满足建设单位对应用系统密码应用的安全需求以及管理要求。
- 根据国家国密改造要求、等级保护（三级）要求三级等保应用系统实施密码应用，侧重应用国密算法加强在身份识别、安全隔离、信息加密、完整性保护、抗抵赖性等方面的安全措施。
- 建立密码应用相关管理制度及运维体系，加强安全管理，统一领导、统一安全策略、统一标准规范、重视安全评估和安全培训，形成一个比较完整的保障体系，切实保障密码应用体系的安全可靠运行。

运营商业务支撑域密码改造方案-某运营商客户项目

业务场景：

目前**运营商的业务支撑域**CRM/**BOSS 等核心系统未实现敏感数据加密存储，大数据平台未实现敏感数据的脱敏访问控制能力，导致敏感数据的管理存在以下安全问题：系统存储层的数据泄露威胁、数据在应用内面临被窃取风险、访问控制被绕过造成数据窃取数据，同时逃避审计系统的跟踪的漏洞以及云上复杂环境带来更多的数据泄露敞口。《网络安全法》、《数据安全法》、《个人信息保护法》也对企业数据安全和个人信息保护提出明确的数据安全合规要求，即使用技术手段对数据和个人信息加以保护，因此使用国产商用密码产品对核心业务系统进行国密算法改造，实现对系统、数据安全保护十分必要。

客户需求：

- 在信息系统建设工程中落实国密算法，根据业务应用系统系统现状，重点解决 CRM、大数据平台中包含的如个人信息等敏感数据，使用密码技术进行存储加密保护的问题，根据不同的数据访问场景进行密钥授权，提升 CRM、大数据平台数据安全防护能力；
- 探索商用密码算法在 IT 领域的可落地场景，提升 IT 安全自主可控，输出可在**集团体系内发布或复制推广的规范标准、解决方案。

解决方案：

- 通过部署数据库加密系统，为系统数据库中对敏感字段以及敏感数据文件提

供动态加解密能力，通过相应后台管理软件设置访问控制策略，并根据权限提供解密范围服务。

- 基于用户权限实现大数据访问安全机制，对大数据平台的敏感数据进行加密/脱敏处理，实现重要数据的机密性和完整性保护，防止数据被非授权人员窃取、篡改。

六、适用行业：

政务、运营商、能源、金融、物联网、车联网等行业。

七、联系人姓名及职位

姓名：庄先生

职位：市场经理

联系方式：18923725603

八、CEO/创始人/总裁/副总裁/联合创始人等对行业发展和甲方的寄语：

不忘初心，牢记使命。密码技术是为了保障公众环境下传递机密信息的科学。信息时代下，密码技术的作用越来越明显。奥联作为密码安全领域的一员，多年来致力于创新的算法研究和应用推广 ,持续为重要领域和新兴产业提供高效、简洁、易用的国产密码技术及产品，满足当今复杂网络环境下的跨应用、跨境、跨平台

等多样化、多场景的数据安全需求。

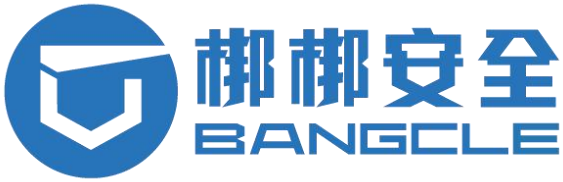
——奥联产品副总裁蔡先勇

梆梆安全

一、公司名称：

北京梆梆安全科技有限公司

二、公司 logo：



三、商用密码产品名称：

1.梆梆密盾密钥安全保护软件

2.可信安全键盘软件

四、产品特点及优势：

特点：

梆梆密盾密钥安全保护软件：

梆梆密盾密钥安全保护软件是完全自主研发的白盒密码技术产品，符合国际白盒数学理论，通过 NIST 密码模块标准化认证，可以保障用户原始密钥在白盒环境

下的存储、使用安全，全过程不出现原始密钥明文，保护用户核心敏感数据。

可信安全键盘软件：

梆梆安全软键盘 SDK 提供一个自定义安全键盘的控件，该控件通过梆梆安全独有的白盒加密技术对密钥进行保护，使用严格的加密方式对用户输入的信息进行安全处理，并提供多种类型的输入字符供用户进行切换，降低了输入数据泄露的风险。

优势：

梆梆密盾密钥安全保护软件：

1.非对称算法支持

作为梆梆安全完全自主研发的白盒密码技术产品，不仅支持全部对称算法的白盒化保护，如：SM4\AES\DES\3DES，同时支持主流非对称算法的白盒化保护，如 RSA\SM2；具备加密、解密、签名、验签功能。

2.算法兼容

所有白盒算法与原有标准加密算法兼容，即客户端使白盒算法加密，服务端可用对应标准算法解密，反之亦可。

3.支持多语言系统

多语言系统支持，包括简体、繁体、英语、韩语等。

可信安全键盘软件：

1.通过商密认证

作为移动应用安全厂商率先获得安全键盘类商密认证的产品，支持各类键盘布局样式，如金额交易数字键盘、证件号码数字键盘等类型。

2.数据全程加密保护

对输入数据进行全程化加密保护，支持国密 SM2、SM4 算法，支持逐字符加密、防截屏录屏等功能。

3.自定义个性化配置

支持对键盘 Logo、标题、位置、按键效果（震动/发音）内容可进行个性化配置。

五、成功案例：

移动金融客户端合规要求-某银行客户项目

业务场景：

银监会、人行等上级监管机构发布强制加密合规性要求，客户自查、第三方检测或被抽查，均不合规。

安全需求：

- 客户安全部需要解决基于中国人行 0092 号文的移动应用的合规监管需求；
- 保护终端密钥和通信密钥安全，防止密钥被非法获取。

解决方案：

- 通过密钥白盒产品为客户 AES、SM4 对称加密算法进行白盒化保护，确保无密钥硬编码和原始密钥明文风险。
- 通过安全键盘为客户解决基于 Android、iOS APP 的支付密码、交易密码等信息输入安全需求。
- 通过 iOS/Android 加固产品为客户提供防逆向工程、二次打包、动态调试等风险，进一步强化保护效果。

高强度数据加密保护-某车企客户项目

业务场景：

某车企旗下各品牌 App 均涉及车控功能，为了保证用户安全，某车企要求对 App 进行高强度安全防护，并通过可信安全键盘软件来提供输入安全保护。

安全需求：

- 针对车企旗下各品牌 App 提供高强度安全防护，为保障应用数据安全和加固性能，采用 SaaS 云服务进行加固，单独划分专用云端资源和管理账号；
- 同时提供 Android、iOS、H5 三个平台的可信安全键盘服务，开发者通过调用安全软键盘 SDK 可以快速、高效的实现逐字符加密、白盒算法、防截

屏录屏等功能，有效保障用户输入安全。

解决方案：

- 保证某车企旗下品牌 App 的安全合规及自身应用安全的要求。
- 通过可信安全键盘软件保护用户基于 H5 页面、iOS、Android 应用的输入数据安全，保护用户的账号、密码、卡号、手机号、身份证号、邮箱地址等敏感信息安全。
- 通过移动应用安全加固保护 Android 应用免遭逆向工程、二次打包、动态调试、数据泄露等风险；利用梆梆安全自主研发的源到源的混淆技术，通过源码加固为 iOS App 提供防逆向、防篡改、防调试等，在不对源码调试和问题排查造成影响的前提下提升源码自身安全性。

六、适用行业：

金融、政府、运营商、互联网、能源、医疗、物联网、车联网等行业。

七、联系人姓名及职位

姓名：翟敏

职位：市场经理

联系方式：18612731019

八、CEO/创始人/总裁/副总裁/联合创始人等对行业发展和甲方的寄语：

随着国家网络安全法制的逐步健全，网络安全已上升为国家战略。作为网络安全企业，在趋势推动、政策引导、内需牵引下梆梆安全自成立之初，就对自身发展及自身要担负的使命责任有相对清晰的认知——梆梆安全开创并繁荣了移动应用蓝海市场，肩负“保护您的软件”重要使命，一直致力于为国家和社会提供有力的网络安全保障，为全球政府、企业、开发者和消费者打造安全、稳固、可信的安全生态环境，为客户提供优质的产品和“一站式”的 App 安全保护解决方案。

——梆梆安全创始人、董事长兼 CEO 阚志刚

北卡科技

一、公司名称：

北卡科技有限公司

二、公司 logo：

三、商用密码产品名称：

北卡密信——专用加密即时通信系统

四、产品特点及优势：

特点：

北卡密信是可快速、私有化部署的专用加密即时通信系统（简称北卡密信(通用版)，其拥有“咔信(政务版)、信令(军队版)、专信(专业版)”等行业版本），客户自主管控服务器，手机安装 APP，只有授权用户才可接入系统，实现全球可达的高强度加密通信，避免黑客的监听与威胁。

具有以下特点：

1、部署私有化：用户完全私有化部署，数据不留存于公用服务器上。

2、服务器防追踪：可快速更换 IP，避免黑客跟踪和攻击。

3、严格的身份认证：采用多重认证技术进行严格的身份认证。

4、国密算法：采用国密算法进行数据加密。

5、敏感信息保护：具有增强的阅时保护与阅后销毁功能。

6、文档安全可控：对文档进行全周期安全管控。

7、加密音视频通话：实现了安全便利的加密语音与视频通话。

优势：

1、私有部署：快速私有化部署，用户自主管控服务器。

2、增强加密：国密算法两层加密（传输层和应用层）。

3、无法追踪：数据包无特征，不易被大数据分析。

4、权威认证：多个国家权威部门认证，资质业界领先。

5、安全打靶：综合安全得分排名第一。

6、端端加密：即使系统管理员也无法查看用户通信内容。

五、成功案例：

客户单位：某政府单位

案例背景：

2022 年 4 月 19 日，中央全面深化改革委员会第二十五次会议审议通过了《关于加强数字政府建设的指导意见》，强调要全面贯彻网络强国战略，把数字技术广泛应用于政府管理服务，推动政府数字化、智能化运行，为推进国家治理体系

和治理能力现代化提供有力支撑。

政务数据涵盖公民、企业、政府部门、社会组织等多个领域的个人敏感信息和重要数据，一旦泄露将会对公民隐私、商业秘密、政府调控决策乃至国家安全造成巨大威胁，因此保障政务数据安全是推进数据治理和数字政府建设的底线。在这样的环境下，守住政务数据安全的前提，又能持续高效办公，是政务单位的第一要务。

近年来，公职人员用微信办公造成信息外泄的事件层出不穷，暴露出在政务工作中使用公用通信系统，存在极大的安全隐患。2021 年 11 月国家保密部门发文，明令禁止党政部门使用微信讨论工作与传文件，并开展清查整顿。客户单位亟需一款移动安全通信系统，能够解决传输工作信息与工作秘密渠道缺乏的问题，实现高效的移动办公与安全通信。

关键挑战：

公职人员使用公用通信系统办公，存在极大的安全隐患。主要表现在：

1、公用通信系统主要用于社交，缺乏严格的身份认证机制，对用户隐私的保护力度不足。工作对象与社交对象同处一个通讯列表，用户容易因为误操作等原因，将工作文档、重要消息误发送至他人，导致外泄等问题。

2、公用通信系统因架构开放、数据明文存储，使用公网进行工作文档、资料的传输，会将文件直接暴露在公网上，容易被黑客攻击窃取，导致工作文档外泄。

3、使用公用通信系统进行重要文件传输，权限管控能力基本为零，文档一旦发送出去，发送方就失去对文档的管控能力，在该平台及对方手机上可长期留存，

无法撤销，被用户随意截屏，泄露后也难以追查。

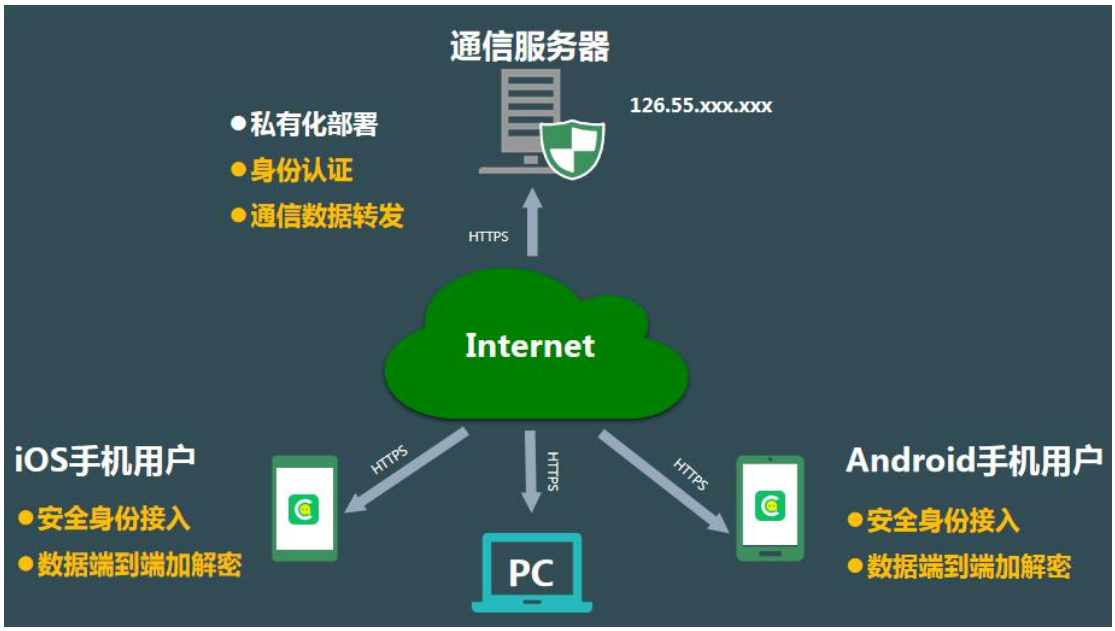
4、由于公用平台服务端存储用户的通信数据且具备解密能力，数据容易被大数据分析，管理员滥用权限、平台被入侵时留存数据等都可能导致用户的数据泄露。

解决方案：

北卡密信政务版——咔信，是一款面向政府部门的、可以快速、私有化部署的专用加密即时通信系统。通过高强度数据加密和严格的身份认证技术实现数据流加密与安全通信；具备安全文档功能，实现文件加密传输、阅读对象可控、文档可追踪；用户可以自主管控通信服务器，数据不会留存在公用的通信系统上。手机上安装“咔信”APP，只有授权用户才可接入系统，实现全球可达的高强度加密通信，避免黑客威胁与机构监听，确保政府部门进行快速、便捷的移动办公与安全通信。

一、系统架构

咔信安全通信系统由通信服务器、移动端手机用户及 PC 端共同构成。



二、核心技术

1、国产密码算法在安全通信领域的深度研究：多年安全通信领域深耕，自主深度掌握相关加密、通信算法，具备国际、国产密码算法研发、改造、优化相关核心技术。

2、通信内容全生命周期防泄防伪防篡技术：自主研发具有国产商密型号的软硬件密码产品，基于国产密码算法的数字证书、数字签名和数据加解密技术，从信道保护、密钥管理、信源端端加密、沙箱防护、一话一密等多个维度确保通信全生命周期防泄、防伪、防篡，为通信提供前向和后向安全保证。

3、具备自主容错能力的弹性架构技术：自研的弹性架构技术，实现了物理部署分布式、逻辑处理分布式、数据管理分布式、系统负载分布式，系统各服务节点松耦合并行运行，具备完善的横向扩展与容错恢复机制，最大限度保证了业务节点和性能的扩展，相比业界其他系统架构，具有高安全、高性能、高容错、易部署、易扩展等特点。

4、自主可控快速私有化部署及智能寻址技术：独有的快速私有化部署技术，可针对各种复杂的网络环境，提供灵活多样的快速部署方案，支持公有云、私有云、独立部署、分级部署及内网、外网和内外网混合部署。

5、基于零信任模型的身份鉴别与访问管控技术：基于自研技术的零信任身份认证与访问管控体系，具备身份认证、信任评估、动态访问控制、业务安全访问等核心安全技术，使系统具有“进不来”、“拿不到”、“看不懂”、“改不了”、“赖不掉”等特性，提供全方位、全生命周期的安全防护。

6、基于国密算法的安全文档及全流程管控技术：自研基于国产密码算法的安全文档数据格式和文档管控技术，可实现文档独立加密、动态授权，分发流转过程、阅读记录可知可控，泄密可溯源。非法用户无法访问和查看文档，合法用户只能在授权访问范围内使用文档，实现了文档“在共享中保护，在保护下共享”。

应用效果：

客户单位表示咔信通过私有化部署实现自主管控，使用国密算法实现数据安全，不仅具备常用通信功能，而且安全文档、阅后即焚、加密通话等特色功能十分出色。通过使用“咔信”，既满足了单位对通信安全性的高需求，又为便利工作开展提供了强有力的支撑，对单位的工作开展具有重要价值。

六、适用行业：

国家重要部门、军队、政府、驻外机构等

七、联系人姓名及职位

联系人：陈小姐

职位：商务

联系方式：18659160309

八、CEO/创始人/总裁/副总裁/联合创始人等对行业发展和甲方的寄语：

随着技术的变革和社会环境的更替，用户通信犹如“裸奔”，网络信息安全面临新的挑战。通信安全之路道阻且长，北卡科技积极响应国家提出的治网主张，着眼于建设网络强国的号召，加强核心技术攻关，采用国密算法，打造出适用于不同行业的加密通信与数据安全解决方案，为国家及国防通信安全保驾护航！

——北卡科技副总经理兼市场总监 周怡

观成科技

一、公司名称：

北京观成科技有限公司

二、公司 logo：

三、商用密码产品名称：

瞰星-密码安全评估系统（ENA）

四、产品特点及优势：

特点：

1. 基于 DPI 的标准加密协议识别

2. 国密算法识别-支持国密算法的识别和验证

3. 基于网络流量分析的密码测评过程

4. 超过 100 余项异常检测

5. 自定义加密业务检测-系统应用未经验证的密码协议或算法

优势：

1. 设备便携，适配多种操作系统

2. 实时/离线两种数据处理方式

3. 评估结果报表自动生成

4. 系统内置数据包分析与原始流量回溯下载

五、成功案例：

某事业单位

六、适用行业：

密码安全测评机构、政企客户

七、联系人姓名及职位

姓名：熊晶晶

职位：市场总监

联系方式：18601343765

八、CEO/创始人/总裁/副总裁/联合创始人等对行业发展和甲方的寄语：

祝愿密码行业蓬勃发展，观成科技用一丝不苟的态度，打造精益求精的密码产品和服务，为国家和民众的信息安全保驾护航。

——观成科技联合创始人 刘燚

国泰网信

一、公司名称：

北京国泰网信科技有限公司

二、公司 logo：

三、商用密码产品名称：

服务器密码机

云服务器密码机

PCI-E 密码卡

IPSec VPN 网关

签名验签服务器

时间戳服务器

智能密码钥匙

云密码服务平台

四、产品特点及优势：

1、服务器密码机

特点：

服务器密码机是一款应用国产商用密码算法（SM1、SM2、SM3、SM4、SM9），自主研制的高性能密码类产品。适用于不同的应用领域，可对应用系统、数据库、存储、网络通信等进行密码加解密安全防护。产品具备加解密、数字签名、身份认证、随机数生成等安全功能。

优势：

1. 支持多密码算法：支持国密算法（SM1 、SM2、SM3、SM4、SM9）及国际通用算法（DES、AES、SHA1、SHA256、RSA、ECC 等 ）。

2. 支持区块链技术应用：可为区块链交易中的用户注册、实名认证、创建交易、验证交易、区块共识、区块确认与同步、区块查询等环节提供基础密码算法服务，

有效支撑采用 PKI 密码体制或标识密码体制的区块链系统密码运行环境安全可靠地运行。

3. 支持多种操作系统：服务器系统支持 Windows 系列、Linux 系列、Oracle Solaris、AIX、HP-UX 等操作系统。

4. 标准接口 :密码机 API 接口符合 GM/T 0018-2012《密码设备应用接口规范》的标准要求，通用性好。

5. 三层密钥结构：采用“系统保护密钥-用户密钥对-会话密钥”的三层密钥保护结构，保证用户密钥及应用系统的安全性。

6. 安全密钥存储：保证关键密钥在任何时候不以明文形式出现在设备外，且密钥备份文件受到主密钥保护。设备机箱被非法开启时，存储的密钥立即销毁。

7. 安全策略：采用基于 IP 地址的白名单访问控制和密钥对一对一的授权码保护机制。

2、云服务器密码机

特点：

云服务器密码机采用容器虚拟化技术，单台可提供至少 100 台虚拟密码机；可提供服务器密码机、金融数据密码机、签名验证服务器等多种类型的虚拟密码机；使用方式与传统密码机基本一致，方便传统业务平滑迁移至云环境。

优势：

1. 密码算法支持：支持全系列国密算法，包括 SM1、SM2、SM3、SM4 等；支持主流的国际密码算法，包括 RSA、3DES、AES、SHA256、SHA512 等。

2. 虚拟化功能：单台云服务器密码机可支持至少 100 台虚拟密码机，每台虚拟密码机可对应用提供独立的密码服务。

3. 多种类虚拟密码机支持：云服务器密码机可支持金融数据密码机、服务器密码机、签名验证服务器等多种类型的虚拟密码机，提供金融数据计算、身份认证（PKI 应用）、签名验签等密码服务功能。

4. 多类型密码接口支持：虚拟密码机具备 JCE、国密 SDF 等多种标准密码应用接口，支持传统应用平滑迁移，满足应用迁入云环境后对密码服务的需求。

5. 虚拟密码机安全服务支持：虚拟密码机支持使用基于国密算法的 SSL 协议建立可信链路，为用户提供安全可靠的密钥管理和密码运算服务。

6. 密码服务高可用支持：云服务器密码机可组建密码机集群，作为密码运算资源池统一对外提供密码服务；支持多台 VSM 组建集群，提供性能更高、可横向伸缩、负载均衡的密码服务。

7. 主流云平台统一管理：通过适配主流云计算管理系统，云服务器密码机可支持无缝接入并接受统一的云平台管理。

3、PCI-E 密码卡

PCI-E 型

mini PCI-E 型

特点：

PCI-E 密码卡是自主研发的高性能基础密码设备 ,能够适用于各类密码安全应用系统中的高速、多任务并行处理密码运算。产品满足应用系统数据的签名验签、加解密需求，并提供安全、完善的密钥管理机制。

优势：

1. 密钥生成与管理：可以生成 256 位 SM2 密钥对，采用物理噪声源产生器芯

片生成随机数。

2. 数据加密和解密：支持 SM1、SM4 等国密标准算法 ECB 和 CBC 模式的数据加密和解密运算。

3. 消息鉴别码的产生和验证：支持基于 SM1、SM4 等算法的 MAC 产生及验证。

4. 数据摘要的产生和验证：支持 SM3 等杂凑算法。

5. 数字签名的产生和验证：可以根据需要利用内部存储的 SM2 密钥对或外部导入 SM2 私钥对请求数据进行数字签名。

6. 数字信封功能：支持基于 SM2 密码算法的数字信封功能，并支持由内部密钥保护到外部密钥保护的数字信封转换功能。

7. 物理随机数的产生：采用物理噪声源产生器芯片生成随机数。

8. 安全密钥存储：采用“设备保护密钥- 用户密钥（卡内 SM2 密钥对/KEK） - 会话密钥”的三层密钥保护结构，保证用户密钥及应用系统的安全性。保证关键密钥在任何时候不以明文形式出现在设备外。

9. 用户访问权限控制：具有用户管理功能，加强密码设备自身的安全性。 基于智能卡的分级使得访问控制更加安全。

10. 可靠的密钥备份机制：备份恢复采用安全可靠的门限秘密共享技术实现备份密钥的分割存放，既保证了备份数据的安全性，也保证了系统备份的可靠性。

11. 支持标准接口：密码卡 API 接口符合 GM/T 0018《密码设备应用接口规范》

标准接口规范，通用性好。

12. 支持内核接口：对于 VPN 等特殊的应用系统，提供了在操作系统内核中调用密码卡的编程接口。接口支持同步和异步调用模式。

13. 标准 PCI-e 高速数据接口：采用标准 PCI-e 通用接口，保证数据高速传输。

14. 支持多种操作系统：可支持 32/64 位的 Windows、Linux、FreeBSD 等操作系统。

4、IPSec VPN 网关

特点：

IPSec VPN 网关基于 IPSec（ Internet Protocol Security）协议为用户提供三层网络数据的保护，提供数据完整性保护、数据源鉴别、载荷机密性和抗重放攻击等安全服务。产品支持实体鉴别方式实现数据源的鉴别，支持国家标准 ISAKMP 协议和 ESP 加密协议实现数据的完整性保护、机密性保护和数据的抗

重放攻击。

优势：

1. 数据完整性保护：使用国家标准的 ISAKMP 协议和 ESP 协议对数据进行安全完整性校验和安全封装，保证数据传输过程中的完整性。

2. 数据源鉴别：使用国家标准的 ISAKMP 协议实现密钥的协商，协商过程采用实体鉴别方式，只有通过实体鉴别的数据包方能被认可。

3. 载荷机密性：使用国家标准的 ISAKMP 协议实现密钥的协商，协商过程严格遵循标准对 SSP 数据进行加密保护，保证载荷的机密性。

4. 抗重放攻击：使用国家标准的 ISAKMP 协议协商密钥，使用 ESP 协议对数据进行安全封装实现抗重放攻击。

5、签名验签服务器

特点：

签名验证服务器是一款主机调用型服务器产品。产品基于 TCP/IP 网络协议实现网络通讯，通过服务器上的管理终端进行相关设置和管理，并为应用系统提供基于《公钥密码基础设施应用技术体系密码设备应用接口规范》要求的数据签名和验签服务。

优势：

1. 标准的规范接口：符合我国电子政务、电商平台、行业信息化系统建设的标准规范及相关国家技术规范要求，为客户的应用系统提供统一的标准接口。

2. 多样化的密码运算方式：支持国际通用密码算法（AES、DES、3DES、IDEA、RSA 等）和国产商用密码算法（SM1、SM2、SM3、SM4 等），实现数据的加解密和签名验签。支持 MD5/SHA1/SHA256/SM3 散列算法和 MAC 的产生及验证。

3. 高速的密码运算能力：基于高性能硬件平台和高速密码运算设备提供极速的密码运算服务，支持国际通用密码算法和国产商用密码算法，全面覆盖主流密码算法。

4. 可靠的自我安全防护：在为上层应用提供安全服务功能的同时充分考虑了自身的安全性设计。物理防护方面采用了防拆、防撬设计，紧急情况下可实现开机毁钥；在密钥管理方面采用密钥注入管理以及密钥在服务器外的备份存放机制，保证了设备和密钥的安全。

5. 全面的兼容适配能力：支持 Windows、SCO UNIX、AIX、HP-UX、Linux 等操作系统平台 API，为各类密码应用服务需求提供支持。

6. 稳定的运行环境 生产环节严格按照ISO9001质量管理体系的流程进行生产、测试、烤机、检验，每一台出厂的机器都经过超 300 小时的烤机和压力测试，系统平均无故障时间（MTBF）大于 30000 小时。

6、时间戳服务器

特点：

时间戳服务器是一款综合使用了公钥加密技术、数字签名、数字证书和数据摘要技术的安全产品，它从国家标准时间发布机构获取标准时间，从第三方可信 CA 机构获得服务器数字证书，为用户的信息数据签发权威、可信的时间戳。产品使用硬件加密卡完成签名操作，具有功耗低，功能全面、性能优越、安全性高、部署使用简便等特点，可广泛应用于安全体系构建中。

优势：

1. 安全密钥存储技术：使用国家密码管理局审批的密码算法和硬件加密设备，使用二级硬件密码模块为安全基础实现密钥管理和密码运算，计算速度更快，安全性更高。

2. 高强度的密码技术：系统支持国家密码管理局指定的 SM2 非对称密钥算法，支持 SHA1、SHA256、SM3 摘要算法，支持 RSA、SM2 密码算法时间戳签发。

3. 成熟规范的设计架构：系统采用业界主流的内部模块架构方式，方便系统模块的组装以及日后的维护、扩展。采用先进的内存检测机制，保证业务服务系统无内存冲突、泄露，保证长期稳定运行。

4. 高兼容性：本产品符合国家标准，兼容国际标准，可与标准时间源、第三方可信 CA 机构等无缝集成。

7、智能密码钥匙

特点：

智能密码钥匙产品是一款具备自主知识产权的、能够满足 PKI 应用的安全产品。该产品严格遵照国密局颁布的 GM/T 0027-2014《智能密码钥匙技术规范》研发。产品兼容多家 CA 证书，支持国内主流 CA 厂商证书应用。支持常用的 Windows、macOS、Linux 操作系统，并兼容麒麟（银河及中标）和统信 UOS 等国产操作系统。

智能密码钥匙可广泛用于各种 PKI 应用的客户端 ,适用于一些对安全性要求较高的行业（比如政府、军队、金融、税务、证券、电子商务等）场景，支持电子商务、电子政务、网络银行、软件和数据保护、系统登录等各种应用。产品拥有完善的上层接口及经验丰富的开发支持团队，可满足各种 PKI 应用的定制化需求。

优势：

1. 密码运算：支持 SM1/2/3/4/7 国密算法，支持 SSF33 国密算法；支持 RSA1024/2048 算法，支持 DES/3DES、AES 算法，支持 SHA-1/256/384 算法，兼容 MD5 算法；对称分组算法支持 ECB、CBC、CFB、OFB 和 CTR 模式。SM1/2/3/4/7 算法标识按照 GM/T 0006-2012《密码应用标识规范》定义。

2. 证书存储：支持 RSA1024/2048 算法的 X.509 数字证书，支持 PKCS#12 格式文件证书导入；支持符合 GM/T 0015-2012《基于 SM2 密码算法的数字证书格式规范》的 SM2 数字证书。

3. 签名验签：支持 RSA1024/2048 的 PKCS#1 签名验签和加密解密；支持 GM/T 0009-2012《SM2 密码算法使用规范》的签名验签和加密解密。

8、云密码服务平台

特点：

云密码服务平台（又称：统一密码服务平台），是云计算技术与身份认证、授权访问、传输加密、存储加密等密码技术的深度融合形成的一种全新密码功能交付模式。平台采用云计算技术架构整合密码产品、密码使用策略、密码服务接口和服务流程，将密码系统设计、部署、运维、管理、计费等组合成一种服务，来解决用户的密码应用需求。

优势：

1. 支持多密码算法：支持国密算法（SM1 、SM2、SM3、SM4、SM9）及国际通用算法（DES、AES、SHA1、SHA256、RSA、ECC 等 ）。

2. 支持区块链技术应用：可为区块链交易中的用户注册、实名认证、创建交易、验证交易、区块共识、区块确认与同步、区块查询等环节提供基础密码算法服务，有效支撑采用 PKI 密码体制或标识密码体制的区块链系统密码运行环境安全可靠地运行。

3. 支持多种操作系统：服务器系统支持 Windows 系列、Linux 系列、Oracle Solaris、AIX、HP-UX 等操作系统。

4. 标准接口 :密码机 API 接口符合 GM/T 0018-2012《密码设备应用接口规范》的标准要求，通用性好。

5. 三层密钥结构：采用“系统保护密钥-用户密钥对-会话密钥”的三层密钥保护结构，保证用户密钥及应用系统的安全性。

6. 安全密钥存储：保证关键密钥在任何时候不以明文形式出现在设备外，且密钥备份文件受到主密钥保护。设备机箱被非法开启时，存储的密钥立即销毁。

7. 安全策略：采用基于 IP 地址的白名单访问控制和密钥对一对一的授权码保护机制。

五、成功案例：

1、国产商用密码应用体系建设解决方案（通用）

项目背景：

根据我国颁布的《密码法》及《商用密码管理条例》相关要求，各类信息系统中涉及密码应用的部分应按照国家密码管理局相关标准要求 ,采用国家商用密码算法 ,采用国密标准的密码应用模式 ,并对应用系统进行相应的合规性建设或改造。

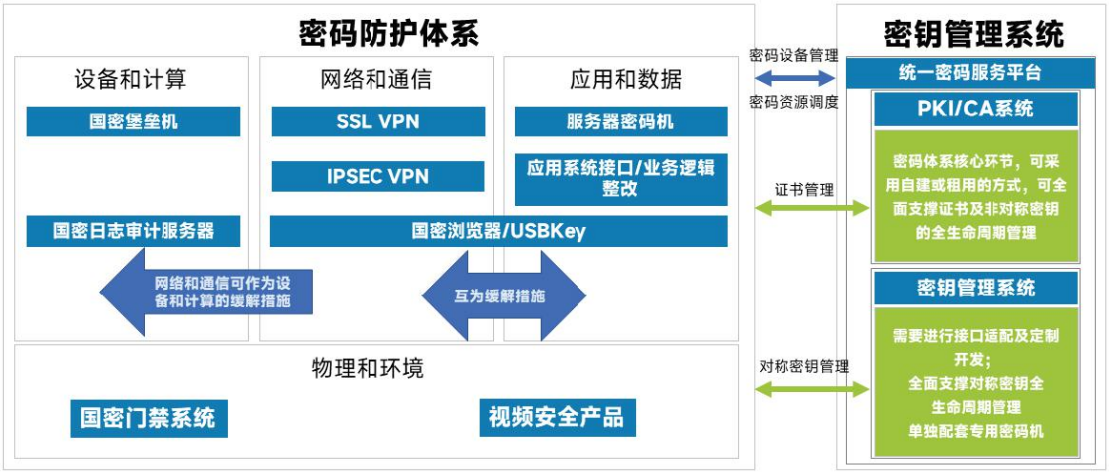
国家密码管理局及其授权机构也将依据 GB/T39786-2021《信息安全技术信息系统密码应用基本要求》针对上述内容进行密码应用测评工作。

方案介绍：

依托于自身具备的多年网络安全及密码领域工作经验，以丰富多样的商用密码产品为核心，以安全集成及定制开发服务为抓手，可以基于信息系统密码应用现状，为用户量身打造一套符合国家密码管理局相关要求的商用密码应用体系。

在商用密码应用体系建设或改造工作前期，公司可对用户商用密码应用现状进行详细调研和评估，充分了解当前密码算法、密码资产和密码应用情况，明确整改环节和整改方法，从而形成完善的应用方案。

在商用密码应用体系实施建设阶段，公司不仅可根据应用方案内容完成商用密码产品的实施部署，也可完成各类商用密码产品相应的服务接口改造工作，同时还可对业务应用系统的业务改造工作进行一定的技术指导，真正做到将商用密码技术融入业务场景，最终帮助用户完成商用密码应用体系合规建设。



方案优势：

1. 完善的商用密码产品体系：自身拥有十余种具备相关资质认证的商用密码产

品，可全面替换各类非国密密码基础设施，且各产品之间可无缝结合，大幅度简化国密改造建设复杂度。

2. 强大的密码应用定制开发能力：自身拥有的各类密码产品全部为自主研发，能够快速响应项目定制化需求，并可为应用系统改造工作提供专业指导。

3. 多行业密码服务接口开发经验积累：具备电力、金融、交通等多行业密码应用相关系统设计、开发与集成建设经验，积累了大量行业标准密码服务接口开发经验，为密码服务接口开发工作提供了有效支撑。

2、某风电场智慧风电网络安全建设方案（电力）

项目背景：

电厂作为能源生产的核心企业，在智能风电项目的建设期间，整体项目的网络安全问题直接关系着整个电厂是否能够并网发电和整个电厂的安全性问题。如果智能风电项目在后期投入运行期间发生网络安全事件，可能会造成基于智能风电项目的相关监测系统误判，将可能导致重大的电力安全事故的发生、国家财产的损失，甚至会危急电厂员工的人生安全。所以电厂在进行智能风电项目的同时如何解决电厂内智能风电相关系统的网络安全防护问题成为了亟待解决的关键。

方案介绍：

根据智慧风电项目各系统前端设备可分为风电场有线专线终端、无线终端、移动终端三类终端设备，针对有线专线终端和无线终端统一通过针对性的终端密码模

组改造实现应用层数据信源加密并同时完成终端设备与电场智慧风电应用系统之间的身份鉴别和完整性校验。

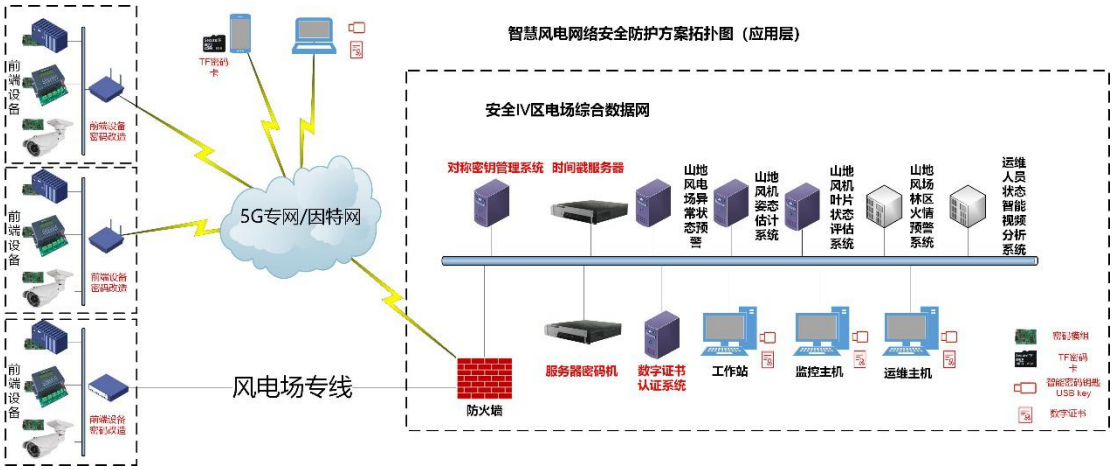
移动终端主要分为移动手机终端及移动 PC 终端，针对手机类移动终端通过手机 APP 的改造并部署 TF 密码卡的方式现实用户移动手机终端 APP 与电场智慧风电应用系统的传输数据加密同时完成用户的身份鉴别和数据完整性校验等基于国产商用密码算法的安全防护工作；

针对移动 PC 终端通过在终端上配套使用签发了基于 PKI/CA 体系的国密数字证书的智能密码钥匙并结合应用系统的改造实现用户移动 PC 终端与电场智慧风电应用系统之间的数据传输加密、完整性校验、用户身份鉴别等安全防护措施。

同时针对内部管理和运维用户同样的是通过在内部终端上部署签发有国密数字证书的智能密码钥匙实现用户终端与电场智慧风电应用系统之间的数据传输加密、完整性校验、用户身份鉴别等安全防护措施。

在电场安全 IV 区综合数据网中部署服务器密码机、时间戳服务器、对称密钥管理系统，同时完成应用系统的安全改造与适配工作之后，应用系统在应用层调用服务器密码机、时间戳服务器、对称密钥管理系统可实现业务相关数据在传输过程中进行加密处理、数据存储中进行加密处理、基于国密算法的完整性校验、用户身份的鉴别、关键数据指令的防篡改等安全功能。

通过部署在电场安全 IV 综合数据网中的数字证书认证系统实现所有终端用户及相关设备的数字证书的申请、注册、签发、注销等证书管理功能，同时保证了数字证书全生命周期的闭环管理。



客户价值：

1. 基于国产商用密码算法对采集的数据进行加密处理，以保证数据的机密性、完整性，同时采用基于国产商用密码的身份鉴别方式对相关设备进行身份鉴别，保证合法设备的安全接入。

2. 针对应用系统的交互场景需要在相关应用系统通信时采用基于国产商用密码算法对传输数据进行加密处理，以保证数据的机密性、完整性，同时采用基于国产商用密码的身份鉴别方式对业务系统进行身份鉴别，保证应用系统相互通信的安全性。

3. 针对应用系统的数据存储场景需要在相关应用系统数据存储时采用基于国产商用密码算法对传输数据进行加密处理，以保证数据的机密性、完整性。

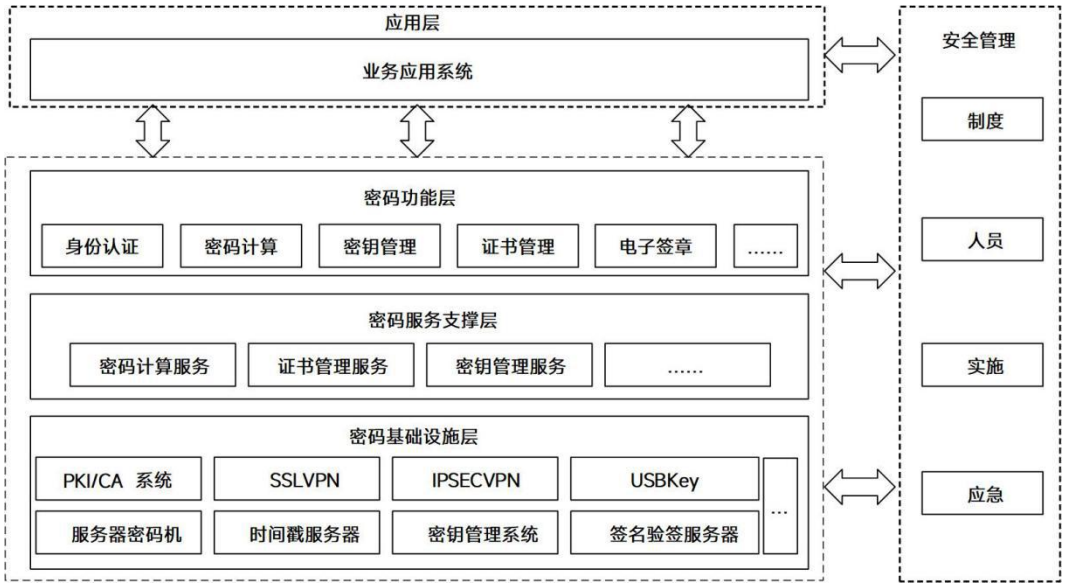
3、某市城运中心商用密码建设项目（政府）

项目背景：

市城运中心用户作为政府单位，主要负责城市运营管理事务，为了满足国家的法律法规及相关标准要求，将密码技术在企业的安全防护体系中正确、合规、有效应用，落实国家要求的同时，加强企业安全防护能力，提高业务系统的安全性、数据的机密性、完整性，操作的不可抵赖性。保证用户的业务办公持续性以及提供全网用户唯一的可信身份。

方案介绍：

结合项目背景及方案总体部署，在满足总体性、完备性、经济性原则的基础上，要通过部署智能密码钥匙（USBKey）、服务器密码机、SSL VPN 网关、时间戳服务器、数字证书认证系统、签名验签服务器、对称密钥管理系统、国密浏览器（内置二级密码模块）、IPSec VPN 网关、时间戳服务器等密码产品，并正确部署配置，以满足本系统的密码应用需求。密码应用保障框架设计如下图所示：



客户价值：

1. 构建基于国产密码算法的密码服务体系，为平台系统及后续其他需要进行国密改造的相关应用提供统一的底层密码服务；

2. 打造国产密码算法的密码服务体系，为平台提供统一的密钥管理、数据加解密、签名验签服务，满足信息系统密码应用的一系列标准；

3. 引入基于 SM 系列算法的数字证书的双因子身份认证体系，提升系统中用户的登录安全级别；

4. 通过国密网关+客户端国密安全模块的方式，构建基于国密 SSL 的应安全传输链路以确保相关工作人员在 PC 侧与业务应用间的通信安全；

5. 通过对相关应用进行国产密码算法改造，实现系统内部敏感信息的存储加密和数据完整性保护。

六、适用行业：

电力、石油石化、能源、轨道交通、政府、金融等行业

七、联系人姓名及职位

姓名：史瑀

职位：品牌运营事业部-总经理

联系方式：13810189202

八、CEO/创始人/总裁/副总裁/联合创始人等对行业发展和甲方的寄语：

随着信息产业高速发展，密码技术作为保障网络与信息安全的核心技术和基础支撑，已成为国家安全的重要战略资源。国泰网信凭借多年密码产品研发和技术创新的经验，持续推动国产密码与业务的深度融合，助力客户构建以密码技术为核心、多种技术相互融合的新网络安全体系，切实构建起坚实可靠的网络安全密码屏障，为客户保驾护航。

——北京国泰网信科技有限公司 CEO 李欣

吉大正元

一、公司名称：

长春吉大正元信息技术股份有限公司

二、公司 logo：

三、商用密码产品名称：

吉大正元密码综合服务管理平台

四、产品特点及优势：

特点：

1.强大的设备整合能力

平台具备整合不同厂商，不同型号密码设备的能力，做到原有设备复用、利旧，保护已有投资。

2.全面的云化服务能力

构建密码资源池，实现云化部署、管理（Docker 镜像模式）;支持平台侧租户管理及租户自管理。

3.全场景密码服务能力

全场景密码供给能力：端侧、网络侧、应用侧

全面的密码服务能力：认证、签验、加解密等

特殊业务场景的服务能力：大数据场景下的本地 SDK 方案、零改造方案等

4.按需分配和弹性扩容能力

采用容器虚拟化技术，实现服务实例的按需分配。

云密码机支持虚拟化，支持弹性扩展。

5.一体化运维和运营能力

使用平台对密码设备进行统一运维、管理、监控等。

面向租户的工单系统，在线受理、审批密码业务。

6.密码可视化和考核能力

密码设备、密码服务运行状态的可视化。

支持多维考核功能，包括应用维、运维维、证书维等，通过考核促进密码的应用。

7.灵活的部署和交付能力

使用云平台资源部署：云平台资源充足

使用硬件服务器部署：云平台资源不足，软件形态交付

一体化服务器（规划中）：云平台资源不足，硬件形态交付

8.XC 环境兼容和适配能力

支持主流 XC 环境，包括信创 CPU、操作系统及数据库。

优势：

1.平台服务架构的扩展性

密码综合服务管理平台可根据客户实际需求进行灵活选择和扩展，在没有较多的密码服务需求时，可以选择性部署平台子系统；或者在当前平台无法满足应用的密码服务需求时，也可以进行集成对应的商用密码产品，扩展平台统一对外提供的密码服务能力。

2.统一、全面的密码服务

密码综合服务管理平台为业务应用提供统一的，全面的密码安全服务，是综合的、完整的体系化的密码管理和服务基础设施解决方案，形成有规范、可靠、完整的密码保障体系，满足企业网络、信息系统、移动应用、物联网等多样化的密码需求。

3.支持多种身份认证模式

密码综合服务管理平台为业务应用提供密码安全服务时，支持多种应用身份认证模式。在认证凭证类型上，平台支持用户名口令、对称密钥/非对称密钥、数字证书等多种凭证进行身份认证，应用可根据其实际情况按需选择合适的凭证类型，

确保应用安全接入平台和使用平台密码安全服务。

4.密码设备的兼容性

支持云密码机、金融密码机、服务器密码机等国密主管部门认可的密码设备，通过国密标准接口进行调用密码设备实现密钥的产生、存储和运算，以及通过相关标准接口进行实现密码设备的统一管理。支持主流密码设备的集成，实现密码设备资源的共享使用和集中管理。

5.可复制性和推广性

微服务一站式运维平台的部署方式，大大降低了产品本身部署的难易程度，并为用户提供可靠的参考方案，在保证了合规性的前提下，充分为客户解决密码应用的问题，更是在政务、能源等方面充分满足客户的需求，解决了管控能力不足、支撑能力薄弱、密码使用复杂度高的难题，并且已经在各部委、央企的应用案例均具有显著的可复制可推广性

五、成功案例：

水利项目建设目标为：实现为水利系统业务中所需签名、加密、认证等提供密钥服务，对水利系统中密钥实现全生命周期监管，保障水利系统密码应用规范性、安全性、密码产品合规性。

本项目以实现国产密码应用一体化管理，面向服务提供快速、集约和统一的密码支撑，减少应用系统使用密码的复杂度，强化密码的统一管控力度为主要任务，最终构建以《密码法》为核心的密码管理和应用安全体系，为水利行业密码应用

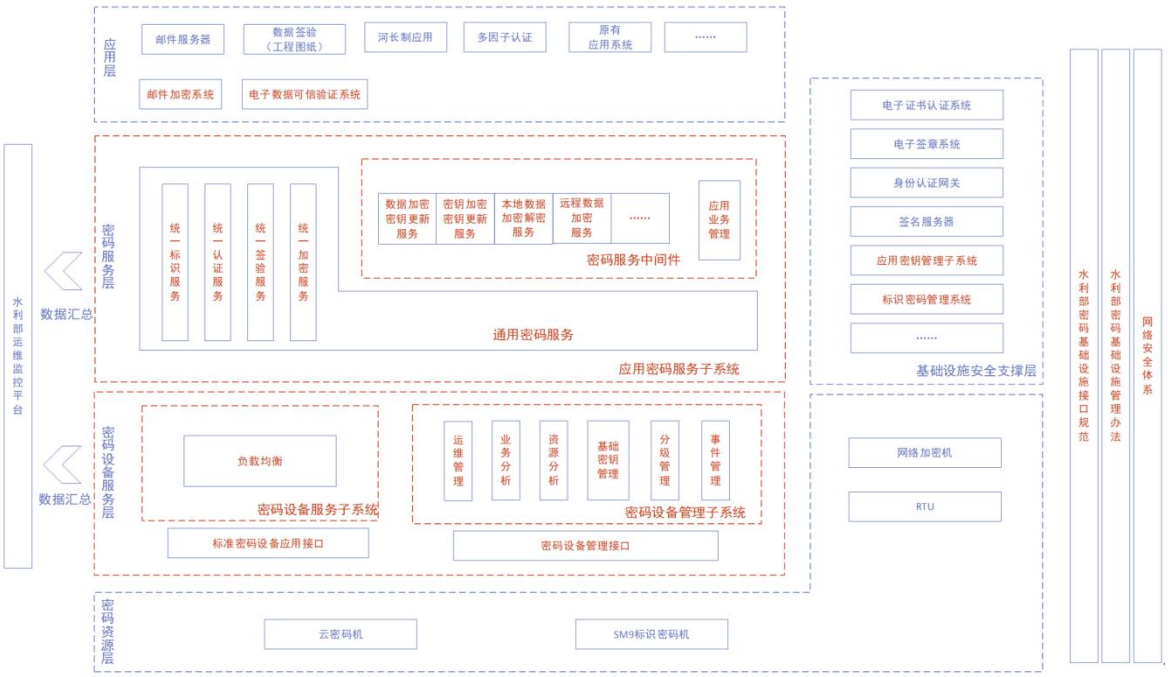
的全面推广、深入应用奠定基础，为水利行业关键信息基础设施安全保驾护航。

本项目完成了水利部密码基础设施的建设，通过密码服务平台进行密码资源的分配、管理和统一调度，实现按需扩展、灵活配置，为部里业务系统按需提供密码运算及密钥管理服务，提升了水利部综合密码安全防护能力。

本项目首先完成了水利部一级密码服务平台和 7 个流域二级密码服务平台的建设，并实现了一二级平台之间数据的打通，达到了部里统览各流域密码服务使用情况的目标，为其它有总分或一二级机构的部委或集团单位等建设级联密码服务平台提供了参考和依据。

本项目使用密码服务平台的虚拟化技术整合底层密码设备资源（密码机、云密码机和 SM9 标识密码机）构建了水利部密码服务资源池，从而能够提供足够的密码服务支撑能力，为水利部各业务系统提供合规的密码服务，同时有了资源池化的能力，从而可以实现更好的弹性扩展和动态扩容。

水利部密码基础设施项目系统总体架构设计上，主要由密码资源层、密码设备服务层、基础设施安全支撑层、密码服务层等四层架构组成，对水利体系内各业务应用提供密码服务支撑，同时以此建设水利部密码网络安全体系、水利部密码基础设施管理办法和接口规范。



1）密码资源层主要由云密码机、SM9 标识密码机等各类密码机组成，主要是负责密钥的生成和存储以及相关的密码运算，支持常见的非对称密码运算和对称密码运算，涵盖国内和国际通用的密码算法。各类密码机可以根据算法的更新和性能提升的要求进行平滑扩容，密码机的增加和退出不影响水利部密码基础设施的统一运转，对于上层应用系统完全透明。

2）密码设备服务层主要由密码设备管理子系统和密码设备服务子系统组成，其中密码设备管理子系统通过统一的密码设备管理接口对云密码机、SM9 标识密码机等设备进行统一的运维管理、业务分析、资源分析、基础密钥管理等；密码设备服务子系统主要是密码资源层之上封装统一的标准密码设备应用接口，为密码服务层和基础设施安全支撑平台提供基础密码服务，同时实现业务负载均衡等功能。

3）基础设施安全支撑层是水利部密码基础设施整体建设的系统支撑层，该层次基于密码设备服务层，结合应用服务相对固化、抽象的密码需求进行凝练和总结，

构建各类密码服务支撑所需的产品和系统，为业务系统提供多元化且符合业务系统需要的密码服务，减少业务系统使用密码算法的复杂度。该层次可以根据业务系统的需求进行动态扩充，增加能够满足业务系统密码应用的需求类型产品，动态提升密码服务的种类、能力和水平。

水利基础设施安全支撑层在水利部原有电子证书认证系统、电子印章系统、身份认证网关、签名服务器之外，补足建设了应用密钥管理子系统、标识密码管理系统，分别对业务系统密钥、基于 SM9 标识算法的密钥进行管理。

4）密码服务层是以密码资源层、密码设备服务层、基础设施安全支撑层为基础，以应用系统对于密码服务的需求为出发点，针对密码设备服务层、基础设施安全支撑平台系统提供的密码服务进行高度抽象、归纳和总结，封装出各类接口服务。密码服务层主要由通用密码服务、典型密码服务和应用业务管理三个模块组成。

在密码资源和密码设备服务层之上，向水利部业务应用提供通用密码服务、典型密码服务和密钥管理服务。通用密码服务是根据水利部的业务应用需要，提供按需、弹性的加解密、完整性验证、签名验签等服务；典型密码服务是基于电子认证基础设施，提供统一认证、单点登录、授权管理、访问控制、电子签章、时间戳等服务；密钥管理服务是基于密钥管理基础设施，提供密钥全生命周期的管理服务。密码服务通常由统一的密码服务中间件供上层应用调用，密码服务中间件对业务应用提供标准接口的统一密码服务，隔离了底层密码设备或服务升级或变更造成的接口变更影响。

- 通用密码服务作为整个密码基础设施平台的原子服务对外提供，结合水利既有业务及后期长远业务建设需求考虑，为上层应用系统提供统一的标识服务、

统一的认证服务、统一的签验服务、统一的加密服务，减轻应用系统对于密码应用的负担，促进密码在水利部外网应用系统的使用。

- 典型密码服务是将水利部一些既有密码应用业务典型密码服务接口封装成中间件，供业务系统进行多样化的密码服务集成调用。在中间件层提供和满足应用系统本地数据加解密、远程数据加解密服务等需求，并且可通过接口服务实现密钥加密密钥、数据加密密钥的更新，减少应用系统直接调用通用密码服务原子功能接口的改造复杂度。

- 应用业务管理针对外部应用接入密码基础设施平台，实现了对应用系统密码服务使用的注册申请、审核、授权以及应用系统具体密码服务接口使用的验证控制等。

密码基础设施各子系统设计了关键业务功能的可扩展性，包括可扩展支持新的密钥类型、新的密码算法、对接新的密码设备等，系统内部模块间交互使用接口进行隔离，保持功能模块低耦合性；系统间交互接口结构定义保持兼容性和灵活性，可以支撑系统将来功能扩展。

密码基础设施内各服务子系统设计支持集群模式部署扩展，当某一类密码服务业务性能不满足应用需求需要进行性能扩展时，平台支持通过在集群节点处增加服务器设备或密码机设备即可实现服务性能的平行扩充，不影响当前平台原有的对外服务状态。

水利部密码基础设施采用自主开发设计方式，深入分析水利部现有的密码应用场景，借鉴其他部委密码应用成功经验，以国家和主管部门法律规范为依据，采用前瞻性的设计思路，整合水利部现有密码设备，以层次化、服务化、松耦合、可

扩展的方式构建水利部密码基础设施框架。针对水利已有密码资源进行升级和定制化开发，按需适当扩充部分密码设备和系统，定制部分管理系统、服务接口和标准规范，为业务系统提供面向服务、可灵活拓展的密码服务支撑。

水利部密码基础设施借助流程设计技术，实现了密码资源在线申请、在线审核、在线分配、在线服务，实现了密码业务的全流程、全在线办理，提高了工作效率；借助于数据报表分析展现技术，将可用密码资源、密码资源调用趋势、密码设备状态、密码服务状态、密码服务调用趋势、应用接入情况、接入单位情况等关键指标的“可视化”，为管理人员提供辅助决策支撑。

六、适用行业：

中央部委、大型能源央企、金融、财政、公安、政务云

七、联系人姓名及职位

姓名：吕姗姗

职位：市场经理

联系方式：13269200306

八、CEO/创始人/总裁/副总裁/联合创始人等对行业发展和甲方的寄语：

密码技术一直是数字经济安全发展的基石，近年来随着政策推动和技术进步，商用密码行业已经开始迈入高速发展期，吉大正元愿与行业和伙伴一起共同进步、守正创新，助力用户数智安全转型，护航数字经济发展！

——吉大正元常务副总裁兼轮值 CEO　田景成

敏捷科技

一、公司名称：

江苏敏捷科技股份有限公司

二、公司 logo：

三、商用密码产品名称：

敏捷数据安全卫士系统 Agile DGS

四、产品特点及优势：

特点：

1. 统一管理：融合集成 DG、DM、DLP、BAK、PSM 等多个安全产品

2. B/S+C/S 架构：由管理平台和客户机组成，管理平台向客户端下发安全管理策略，客户端执行相应的动作

3. 用户管理：根据实际的用户密级和岗级的划分来更改数据字典的用户密级、

岗级的值域范围；

4. 权限管控：采用 RBAC 基于角色的权限访问控制机制，权限需分配到角色；

5. 授权管理：根据用户购买的系统功能模块、点数提供系统授权文件，通过导入授权文件可获得系统相应模块的使用权限；

6. 域同步管理：将系统与域服务相结合，将域服务所有组织机构、部门、账号同步到系统中，通过域账号登陆系统；

7. 工作流定义：以实现单级、多级的文件外发审批流程。

优势：

原创防破解技术、集中式部署、支持多种操作系统、信创适配、电子文件全生命周期统一防护管理、与内部应用系统集成性良好、多模块灵活扩展、透明加密无感知、不改变原有架构和办公操作、大文件处理能力出众、完备的日志统计、安装维护非常简单。

五、成功案例：

中国中车、一汽集团、长安汽车、东风汽车、中信泰富特钢、苏交科、天合光能、紫金山实验室、泸州老窖等。

客户需求：

中车株洲电力机车研究所有限公司（中车株所）始创于 1959 年，属于轨交行业。

前身是铁道部株洲电力机车研究所，现为中国中车股份有限公司一级全资子公司。目前已经建成涵盖轨道交通及工业领域大数据存储管理与分析挖掘业务，可支持海量工业设备数据接入的大数据平台，实现了打通设计、制造、物流、售后、质量等各个领域的关键数据，并形成闭环，产生服务价值。然而，轨道交通行业的特点是资产密集、长周期运营，而且信息非常分散，这就导致它对产品的质量和安全方面要求比较高。中车株所在追求企业转型升级的同时，对工控系统安全的认识达到了一个新的高度。积极推进企业级系统集成，实现生产和经营的无缝集成和上下游企业间的信息共享，开展基于横向价值网络的协同创新，在企业间的设计协同、制造协同方面逐步由原来的纸质信息传递，转变为以三维设计模型为核心的电子文件交换，带来了便利的同时，也带来了商业秘密泄露、图纸数据随意篡改、电子文件残留等数据安全风险。

项目实施：

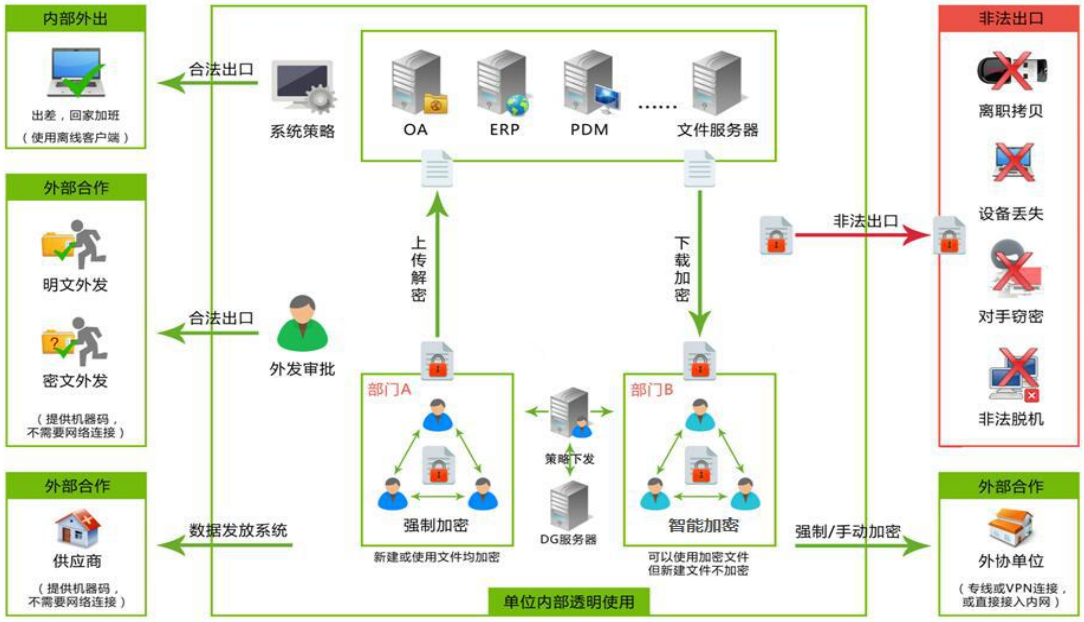
中车株所数据加密防泄漏项目通过敏捷科技自主研发的数据安全卫士系统 Agile DGS，在工业互联网体系架构的基础上应用了基于工业控制系统的防护手段，针对工业设计数据面临的威胁，借助敏捷科技核心专利技术“电子文件安全标签”、“高速高通云存储加密技术”，基于我国密码标准算法构建，通过阅后即焚、安全云盘、数字签名、透明加密等功能，构建了面向工业设计数据全生命周期安全管理的解决方案，确保中车株所智能制造数据集中管控的同时实现安全可靠管理，有效保护中车株所的核心资产、知识产权及其它相关数据。

（1）终端数据智能安全防护：包括数据智能安全子系统、终端虚拟化桌面子系

统、终端桌面安全子系统、终端外设控制子系统、文件透明加密子系统等五个子系统，有效防止机密信息泄漏。

（2）网络数据安全防护：提供虚拟安全网络子系统，确保具体业务应用系统环境的专用性和“干净性”，实现了基于具体业务应用系统的动态“专网专用”，也从安全管理角度上对网络数据进行安全精细化管理。

（3）平台数据及因公外出数据使用安全管控防护：实现对移动设备在外使用过程中全程保护，有效的杜绝外出人员主动和被动的数据泄密，实现了外出移动设备的授权使用、安全认证和电子文件的便捷高效、安全可用。



项目成效：

1、提高中车株所工业互联网系统信息安全防护能力和高效协同管理水平。

对系统敏感数据进行智能识别、分级加密、权限管控，全方位提高自身信息安全管控能力，有效解决中车株所内部合法用户有意或者无意的信息泄漏。

2、满足合规性要求

满足工信部《工业控制系统信息安全行动计划（2018-2020 年）》及相关指南要求，落实工控系统常态化检查评估、风险通报、事件应急等工作，同时加强工控系统使用人员的安全意识及技能培训。

3、数字中车战略目标的契合

集团先后对各子公司开展了安全性评价标准查评，并与敏捷科技合作，对系统进行数据防泄漏体系建设工作。

实现了企业内部及产业上下游、跨领域生产设备与信息系统的互联互通、资源共享、数据集成安全共享，提高了企业数据安全防御能力，推动株洲的轨道交通产业，企业与企业之间、企业与政府之间的良性互动，为促进全国工业互联网行业持续健康发展提供有力支撑。

六、适用行业：

智能制造、医药、能源、轨交、设计院、半导体、金融、地产、教育、运营商等

七、联系人姓名及职位

姓名：王宇佳

职位：市场助理

联系方式：15852924320（微信同号）

八、CEO/创始人/总裁/副总裁/联合创始人等对行业发展和甲方的寄语：

释放数据价值、让数据更安全——敏捷科技副总裁 倪海燕

明朝万达

一、公司名称：

北京明朝万达科技股份有限公司

二、公司 logo：

三、商用密码产品名称：

Chinasec（安元）数据安全管理系统

四、产品特点及优势：

特点：

Chinasec（安元）数据安全管理系统，以“防内为主、内外兼防”为理念，通过认证、加密、监控、追踪等手段，对传统 PC 终端和移动终端提供文档加密、身份认证、安全接入、应用保护、访问控制等全方位的安全防护。

采用 C/S 架构和 B/S 架构相结合，内外网互通的架构思路，对网络安全和数

据安全提供全 IT 架构的多套解决方案，针对敏感数据提供全生命周期的安全管理和审计。将安全防护贯穿于数据产生、访问、传输、使用和销毁的过程中，真正实现事前安全管理、事后行为审计。

优势：

1、以数据加密技术为核心

支持 PKI 体系数字证书，支持国密 SM1 、 SM2 、 SM3 及 SM4 等算法，兼容国际主流标准。密钥体系严格遵守国家商用密码规范要求，并通过了国家保密局、国家密码管理局等权威机构的认定。

2、以终端文档内容发现为管控依据

支持终端文档根据预先定义的规则对文档进行内容扫描，并最终确定文档是否包含敏感信息。支持的文档扫描规则类型包括：关键字、正则表达式、文档分类特征与文档指纹。支持对终端本地存储的文档进行全盘智能扫描，支持对外发的文档进行即时内容扫描。为后续的管控手段提供依据。

3、全 IT 架构统一管理

可实现对各种类型终端的统一管理，有效应对企业 IT 架构的快速变革与延伸，实现全 IT 架构下数据安全的协调联动管理和异构终端统一化管理。

4、高效可配置的部署模式

支持服务器的集群部署，同时平台中的业务服务器、数据库服务器、文档服务器和日志服务器等均可进行单独部署。

5、与现有业务系统灵活对接

采用层次化的设计，实现了高扩展性，支持企业现有的各种标准接口，并提供跨平台、多层次的安全中间件，通过安全中间件可与企业现有平台上的各种业务系统进行安全无缝结合，不改变、不影响企业既有业务系统的正常运作流程。

五、成功案例：

案例一：国内某大型国有银行

采用 Chinasec（安元）数据安全管理系统终端数据防泄漏解决方案。实现的功能主要包括：

对终端电脑进行屏幕和文档水印内容的展示；支持显示文字、二维码、图片水印。

实现对终端文件打印行为进行审计与管控处理，支持对打印的文档内容进行扫描，并根据扫描的结果来判定是否对待打印的文档添加打印水印或者禁止打印。

实现对终端存储的全盘文档进行内容扫描，发现用户终端存储的敏感数据文件，帮助企业梳理敏感数据资产的分布。

实现对终端移动存储设备的全生命周期管理功能，支持对移动存储设备拷入文件自动加密，拷出文件自动解密的安全读写管控。

实现对通过共享网络、即时通讯软件工具的外发途径外发文件时进行文档内容扫描和审计管控。

项目通过上述数据安全管控手段在不影响用户正常办公的同时，防止企业敏感数

据泄漏。

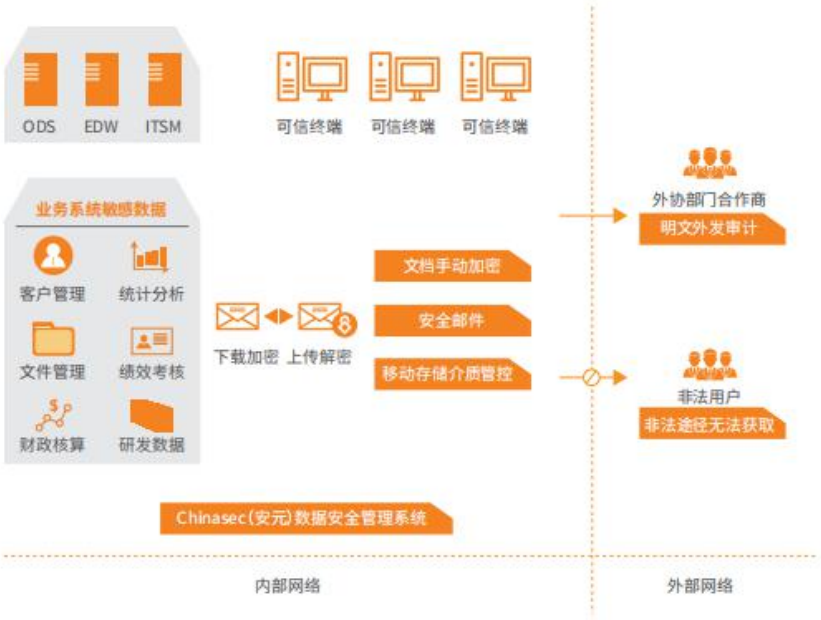
案例二：国内某大型电信公司

采用 Chinasec（安元）数据安全管理系统，提供数据全生命周期防护解决方案，员工从业务系统下载的敏感文档在企业内部以密文的形式流转，终端边界管控策略则保证了非法途径无法获取、无法解密敏感文档。

应用保护：业务系统敏感文档下载自动加密，上传自动解密。

终端防护：通过文档手动加密、邮件加密、移动存储介质加密来保证敏感文档不会泄漏到外部网络。

明文外发审计：审计或审批后的文档允许以明文的形式发送到外部网络，为办公提供便捷通道。



六、适用行业：

全行业通用，也可针对不同的行业制定具体的解决方案。

行业包含：金融、公安、政企、智联汽车、工业、医疗等

七、联系人姓名及职位

姓名：刘京扬

职位：市场经理

联系方式：18500653885

八、CEO/创始人/总裁/副总裁/联合创始人等对行业发展和甲方的寄语：

行业寄语：数据安全离不开持续创新，持续创新构建核心竞争力

——北京明朝万达科技股份有限公司 董事长兼总裁-王志海

宁盾

一、公司名称：

上海宁盾信息科技有限公司

二、公司 logo：

三、商用密码产品名称：

宁盾多因素认证（MFA）

四、产品特点及优势：

特点：

移动办公入口（VPN、虚拟桌面）、业务系统登录入口（office365、outlook）、网络接入、数据中心基础设施登录入口等全场景适用，有本地部署和云服务两种选择。

优势：

1. 全场景覆盖：移动办公登录入口（VPN、虚拟化桌面、云桌面接入）、业务系统登录入口（Office 365、Outlook 邮箱、泛微 OA 等）、有线无线网络接入、服务器/堡垒机等基础设施登录入口，都可以使用宁盾多因素认证。

2. 令牌形式丰富：手机 APP 令牌、硬件令牌、短信令牌、邮件令牌、企业微信/飞书/钉钉工作台中的 H5 令牌、小程序令牌、推送认证、扫一扫认证，并兼容 RSA、Google 第三方令牌，企业根据自身需求任意选择。

3. 认证策略灵活：可基于角色、部门等多种属性进行条件组合，匹配实际使用场景。

4. 多账号源兼容：快速对接各种应用系统及对接标准和自定义账号源（如 AD、LDAP、POP3、HTTP 等），无需改造现有应用的账号管理方式下，实现多应用统一多因素认证。

5. 与业务无缝衔接：5 种令牌派发激活方式；分钟级部署上线，根据业务需要逐步推进使用。

6. 快速实现合规：国密 SM3 杂凑算法，拥有国密、商密资质。

7. 用户自服务平台：用户可自助解绑、找回令牌，无需 IT 管理员协助，减轻运维压力。

五、成功案例：

【案例一】某国有银行：

所属行业：金融行业

客户需求：

该银行目前在用的 Web 应用、用友 U8 业务系统及 Citrix 虚拟桌面、山石网科 VPN、堡垒机、服务器都采用 AD 域账号和静态密码的方式进行登录访问。随着业务系统数量不断增多，弱密码问题逐渐暴露，容易引发安全危机。因此，需要为业务系统及 VPN、堡垒机、服务器等设备的登录访问进行安全加固，降低因弱密码问题引起的安全风险。

解决方案：

业务系统通过安装相应的代理软件及配置，与部署在公网或内网的宁盾 AM 认证服务器进行通信，实现业务系统登陆增加二次动态口令身份认证。采用 DKEY Agent 和配置 Radius 方法集成，十分方便多业务系统接入，无需二次开发，减少整体项目实施风险，节约成本。

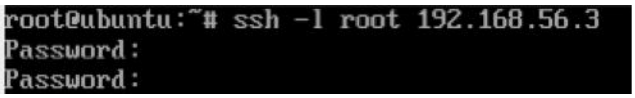
虚拟桌面、VPN、堡垒机、服务器的多因素认证则只需简单配置，将认证指向宁盾 AM 即可。

使用效果：

在业务系统及设备上启用宁盾多因素认证后，用户输入完 AD 域账号和静态密码后，需要再次输入动态密码进行身份认证，双重认证增强了用户身份安全，降低因弱密码问题而引起的攻击风险。

业务系统登录流程：采用单步认证，在密码框内输入静态密码+一次性动态口令

Linux/Unix 服务器登录：以 ROOT 用户为例，连接 SSH，在第一次提示输入密码时输入该用户的静态密码 ,在第二次提示输入密码时输入该用户绑定的令牌的动态密码。



山石网科 VPN 登录：

客户收益：

- 满足了国家等保要求
- 网络设备管理实现了统一身份认证并针对不同帐号设定不同权限，有效的控制了帐号的泄漏与共享，使登录操作可以实名追溯。
- 通过纯软件配置方式 ,满足业务系统集成动态口令诉求 ,具有良好的扩展性，节省部署成本。
- 支持多系统同时接入动态密码认证，并分配不同认证策略，有效降低管理及部署成本；

【案例二】某互联网头部企业

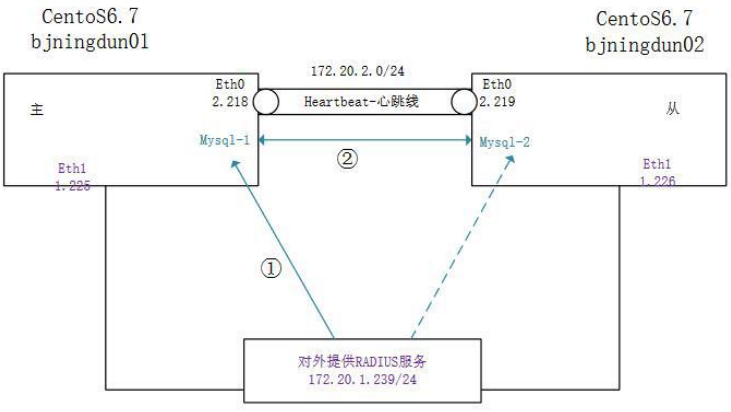
所属行业：互联网

客户需求：

- 实现邮件系统（OWA）多因素认证。用浏览器访问 OWA 系统后，在出现的登录框中输入邮件帐号和密码，在二次弹窗中输入动态密码；
- SSL VPN 采用动态密码密码认证，AD 结合完成多因素认证
- 单点登录 SSO 系统实现多因素认证；
- 登录堡垒机实现多因素认证。

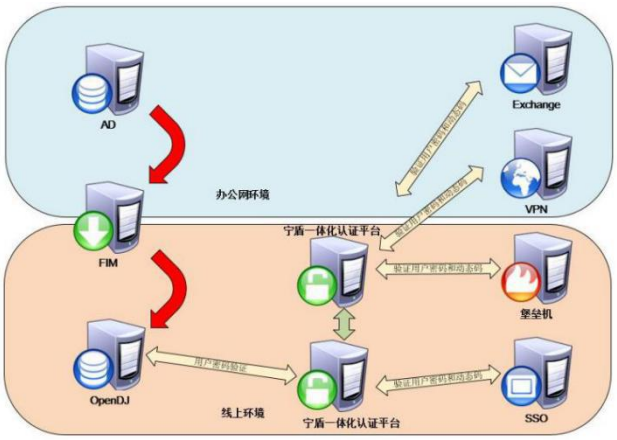
解决方案：

在 2 台服务器上安装宁盾一体化认证平台，采用高可靠部署方式，统一管控员工 OWA、VPN、SSO 等系统的多因素认证登录，具体实现方式如下图：

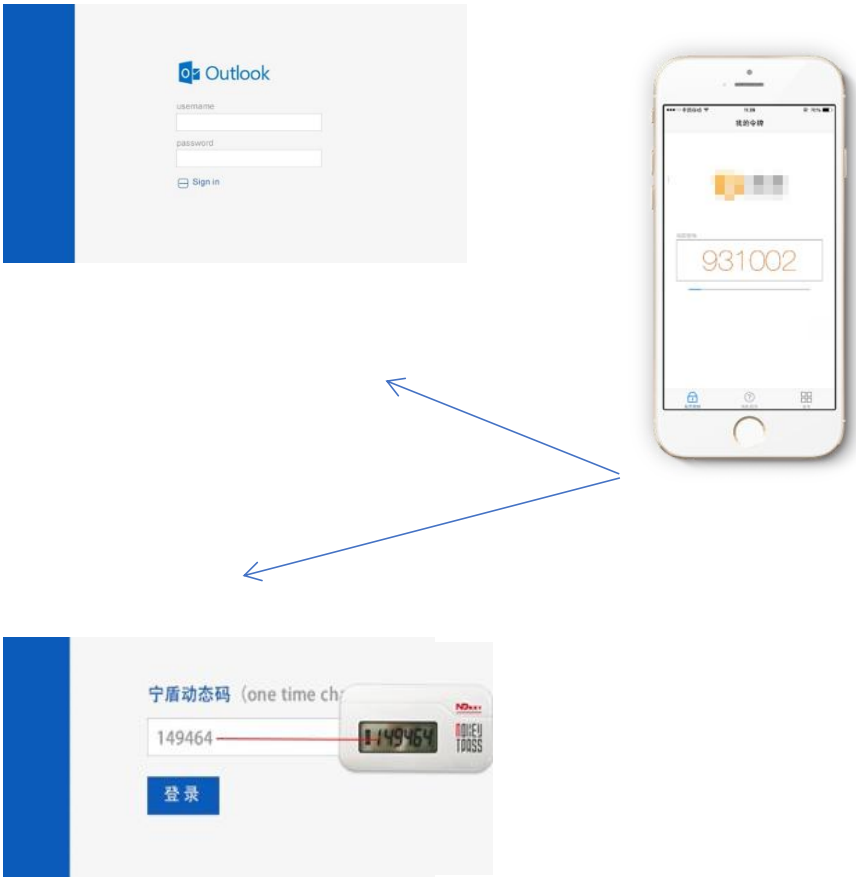


网络拓扑：

项目中主要产品有宁盾一体化认证平台、AD 系统、OpenDJ、Exchange OWA、SSL VPN、SSO、堡垒机等。



使用效果：



员工登录 OWA、VPN 以及网关人员登录堡垒机时只需在输入静态密码后，再次输入宁盾手机 APP 令牌中的动态密码即可开启二次认证。

客户收益：

- 兼容多品牌设备，而且兼容多账号源认证体系，实现对多业务系统、多品牌设备、多源账号的统一多因素认证，提供了对上万个帐号的双重保护和统一管理，还为设备带来轻量化的安全管控；
- 针对员工和设备下发数千个手机令牌、硬件令牌，采用批量式派发和回收的管理方式，不但提高了工作效率，而且大大减少了人员调动带来的运维成本；
- 针对 Exchange OWA 等系统进行定制化开发，既可以单步认证，也可以多步认证；
- 采用高可靠式部署为该企业的账号管理提供稳定、安全的服务环境；
- 轻量级一体化认证平台，不但操作更加方便，而且易于维护。

六、适用行业：

金融、政府、医疗、制造业、科技互联网、教育、商业地产、交通物流等全行业

七、联系人姓名及职位

姓名：宁宁

职位：宁盾市场部

联系方式：400-658-2855

八、CEO/创始人/总裁/副总裁/联合创始人等对行业发展和甲方的寄语：

身份是企业数字化的基石，身份安全才能确保数据安全、业务安全。宁盾作为身份管理厂商，自成立以来，始终注重与上下游厂商的生态合作，致力于以第三方厂商的开放性、兼容性，更好地服务于千行百业，构建普惠的身份管理。

——宁盾 CEO：刘英戈

时代亿信

一、公司名称：

北京时代亿信科技股份有限公司

二、公司 logo：

三、商用密码产品名称：

1. 时代亿信安全电子邮件系统
2. 时代亿信电子文档安全管理系统
3. 时代亿信 UAP 数字证书统一认证系统
4. 时代亿信密钥管理系统
5. 时代亿信 ETCA 数字证书认证系统
6. 时代亿信签名验签服务器
7. 时代亿信 VPN 安全网关

8. 时代亿信 UAP 安全认证网关

9. 时代亿信服务器密码机

以上产品均已获得商用密码产品认证证书，符合等保要求，满足密码应用安全性评估要求。

四、产品特点及优势：

特点：

1. 产品均采用国产密码算法，已经全部取得国家密码局商用密码产品认证证书，符合密码应用安全性评估要求，符合等保要求；

2. 支持信创和非信创环境混合部署，可实现用户平滑过渡；

3. 产品已经获得规模化应用验证，大用户量并发访问下运行稳定、可靠。

优势：

1. 拥有完整的软件、硬件密码产品线，可为用户提供一站式密评、密改解决方案服务；

2. 先后助力党政、运营商、能源等行业客户完成密码应用上线及密评验收，实践经验丰富；

3. 具备覆盖全国县乡级的技术服务体系，可提供完善的本地化服务。

五、成功案例：

成功案例：某国家部委商用密码改造

用户具有多个互联网业务系统，为公众及行业用户提供服务。由于系统建设年代早，没有统一规划，每个业务系统的身份鉴别、数据传输、数据存储等关键环节绝大部分没有使用密码技术进行保护，部分使用了密码技术的业务应用，也使用的是 RSA 等外国密码算法。

为了满足国家密码法律和相关信息安全政策要求，需要对不符合要求的密码算法进行更换，对未采取密码技术的业务应用进行升级改造。

时代亿信通过统一密码服务平台及配套的国产密码基础设施，为用户的互联网业务系统提供身份鉴别、数据传输安全、数据存储安全、完整性保护、抗抵赖性等方面的密码防护，为互联网业务系统的安全可靠运行提供全面的密码支撑服务。时代亿信统一密码服务平台适配各类服务器密码机、签名验签服务器、时间戳服务器、密码卡、智能密码钥匙等密码设施设备，屏蔽了不同密码设施设备的接口差异，通过统一的密码服务接口，为用户各类互联网业务系统提供标准的国产密码算法调用服务，满足密码应用安全性评估要求。

六、适用行业：

党政、金融、能源、央企等需要进行密码安全性应用评估的行业等。

七、联系人姓名及职位

姓名：魏海娜

职位：品牌生态经理

联系方式：13811021962

八、CEO/创始人/总裁/副总裁/联合创始人等对行业发展和甲方的寄语：

密码技术是网络安全的核心支撑，是国家的重要战略资源，国产密码算法则是保障信息安全与自主的基础支撑，时代亿信愿与更多的上下游生态合作伙伴，强强联手、共同推进国产密码算法的广泛应用，促进更多行业用上密码、用全密码、用好密码！

——时代亿信副总裁 杨学静

双湃智安

一、公司名称：

北京双湃智安科技有限公司

二、公司 logo：

三、商用密码产品名称：

双湃数控系统商用密码应用攻防靶场

四、产品特点及优势：

特点：

1. 传输安全：通过密码模块与数控系统结合实现数控系统密码计算能力，在远程管理过程中通过多重安全防护机制和认证机制，保障远程信令传输的安全性。

2. 密码应用一体化系统部署：基于高性能硬件平台和专用密码运算单元打造，

集成计算资源虚拟化、网络虚拟化　密码应用服务虚拟化，提供虚拟化的密码系统。

3. 移动协同签名技术：通过协同签名技术实现智能移动密码应用安全性和合规性，私钥不落地存储，通过派生因子加算法与服务端私钥片段计算合成，生成完整私钥；移动端智能密码模块（SDK）具备国家密码管理局颁发的软件二级模块资质，符合 GB/T 39786 三级要求。

4. 数据安全：数控系统加工文件是生产制造企业的核心数字资产，数控系统应用商用密码技术保障在各环境流转中文件不被篡改、加密传输，保障文件的真实性、有效性、可用性、安全性，保障文件不被窃取。

5. 身份认证安全性：以数字证书为信任源点，通过数字证书为信任域内的设备、人员进行身份鉴别；支撑平台部署统一身份认证系统、通过统一身份认证系统与密码应用结合，实现前端人员的身份鉴别、授权管理、行为审计、单点登录等功能。

6. 国密算法：采用云架构虚拟化部署，全线产品、密码服务采用国密算法实现，符合 GB/T 39786 密码算法使用要求。

优势：

1. 弹性产品架构：产品具备全部自主知识产权的引擎层、中台层、应用层三层架构，运行稳定可靠，支持快速扩展应用层功能。

2. 高仿真场景还原：产品支持设备仿真、网络仿真以及实物接入，满足不同业

务场景下的网络架构还原，彻底脱离虚拟化、云计算技术体系，形成独具特色的网络安全仿真应用类支撑平台。

3. 专业节点与拓扑构建工具：配套全自主可控领先技术的专业级仿真网络可视化构建工具，让用户能够完全复现真实的网络架构。

4. 独具特色的虚实结合防御训练支撑技术：产品可以接入各类工业设备、控制系统、已适配大量 NFV 网络安全设备，结合自动化攻击机器人、触发器等，支撑各类商用密码、网络安全、防御技术训练。

5. 科学有效的评估体系：基于 X-CAPTURE 技术，实现全量数据采集，系统结合资产模型、TKS 能力画像模型，对活动参演方进行效能评估。

6. 自定义态势编排：产品提供个性化态势编排器，支持用户的个性化态势效果设计和编排，满足多场景、多业务、多维度的态势呈现需求。

7. 前瞻性的核心技术支撑：Meta computing、AI 赋能的流量发生、全自动攻击流程编排。

五、成功案例：

案例一：海尔通用网络培训系统

结合项目背景需求，为用户打造集仿真训练、比武竞技、实操培训为一体的实训竞技平台。通过技能评估模型、能力画像模型、裁决引擎、可视化引擎等技术，为攻防人才培养、技术水平评定、人才选拔等提供训练场地。主要功能如下：

教学培训：提供集中化培训与学习场地，内置专业理论学习教学资源。

实战训练：提供隔离的实战训练场景，内置 1000+实训课程。

竞技比赛：提供竞赛试题与构建场地，内置 300 道 CTF 题目。

人员评估：提供人员评估模型，完成人员技能分析和人员画像输出。

案例二：沈阳理工大学网络安全仿真系统

结合项目建设需求，构建专项测试评估系统平台，为用户提供场景还原、设备测试、威胁评估、数据分析等技术能力，实现真实业务系统的还原与复刻、测试环境的下派与跟踪、测试报告的编辑与汇总，通过预置触发器引擎实现真实业务流量、事件的模拟触发，达到高仿真模拟及测试需求。主要功能如下：

业务还原仿真：搭载专业级拓扑构建工具，实现真实的业务网络构建与还原。

评估模型构建：提供评估模型构建工具，实现评估用例的编辑与定义。

事件触发模拟：提供流量重放、自动化事件编排工具，实现流量与事件的定时触发与手动触发，高度还原真实业务场景。

评估分析输出：提供测试评估场地，实现被测目标的资源启动与测试，支持测试的结果汇总分析及结果输出。

案例三：网安协会-设备测试

为用户提供工控相关设备测试环境，提供工控相关协议模拟仿真，实现工控安全

设备的评估与测试。包括工控防火墙测试、工控堡垒机测试、主机卫士测试、IDS 测试、USB 防护测试、商用密码应用测试。

六、适用行业：

制造业、信息传输、软件和信息技术服务业。

七、联系人姓名及职位

姓名：任浩源

职位：市场总监

联系方式：18610940906，renhaoyuan@dualpi.com

八、CEO/创始人/总裁/副总裁/联合创始人等对行业发展和甲方的寄语：

高档数控系统作为公司一个重要发展方向，随之带来的数控系统网络化和基于工业互联网全新的“云-边-端”的新业务应用模式也带来了新的安全挑战，公司需要建立网络安全信任体系来消除潜在的安全威胁，保证资源的可靠性和数据的完整性，保障未来数控私有云部署实施和业务的开展。

数控系统商用密码应用攻防靶场以数控系统研发生产和推广应用能力、商用密码研究和应用能力以及标准制定和测评认证能力为基础，立足于现有的产品和技术

储备，构建数控系统信息安全防护中的密码应用指南及解决方案，该方案由云端密码服务平台、数控系统基础安全防护、商密安全增强数控系统和商密安全增强机器人控制系统几个主要模块组成，该解决方案可以有效解决数控系统目前面临的“缺加密、无防护、少认证、弱授权”的问题，并将相关产品量产并推广应用，将密码技术应用到数控系统的开发、集成和应用之中，基于商用密码的整体数控安全解决方案在制造业大规模推广应用，将形成完整的数控系统信息安全产业生态。

——CEO/首席科学家　陶耀东

新华三

一、公司名称：

新华三集团

二、公司 logo：

三、商用密码产品名称：

新华三商用密码应用安全性评估解决方案

四、产品特点及优势：

新华三商用密码应用安全性评估解决方案针对密码应用相关标准规范，基于物理环境安全、网络和通信安全、设备和计算安全、应用和数据安全、密钥管理安全角度进行统一规划和设计，新华三自有商密产品为基础，充分整合密码应用需求，帮助用户建立一套安全、合规、完整、有效的密码应用体系；方案符合 GB/T39786-2021《信息安全技术信息系统密码应用基本要求》中对于不同等级

信息系统的密码应用要求。

云网安全面融合：底座云平台、网络资源、计算资源、存储资源已与密码产品完成对接，具备国密能力，提供多种密码安全服务，形成“云网安”一体化的能力。

一站获取完整密码产品：具备自主研发的密码产品家族，同时通过多样化的生态合作伙伴为客户提供全方面的密评改造能力。

合规设计与专业咨询团队：具备多位经验丰富的持证密评师和专业的密评方案交付团队，提供全流程的专业密评服务；基于 GB/T39786-2021 标准设计，系统建设资源优化部署，可落地性强，满足用户一次性过密评的需求。

五、成功案例：

淮安市智慧城市密码改造项目

淮安政务云为数百万市民提供便捷数字生活保障。在《密码法》、在国标《信息安全技术信息系统密码应用基本要求》（GB/T 39786-2021）、《国家政务信息化项目建设管理办法》等政策法规的要求下，淮安政务云和大数据业务系统启动整体商密改造，以满足国家政策合规要求，并为未来数年的业务安全发展做充分准备和支撑。

新华三项目组通过前期咨询调研、差距分析、密码应用方案设计和实施，助力淮安政务云顺利完成密码改造。江苏省信息安全测评中心从物理和环境、网络和通信、设备和计算、应用和数据以及密码管理制度方面进行了详细测评，并出具商

用密码应用安全性评估符合报告，顺利通过了商用密码评估。

通过淮安政务云密码改造，为淮安政务系统提供符合国密要求密码安全能力，保障政务数据生命周期安全中结构化数据、非结构化数据存储加密安全；提供密钥管理、数字证书、签名验签等灵活的密码服务，实现云平台和商用密码技术的融合，促进数字政府、“互联网+政务服务”、新基建、物联网、智慧城市等领域的融合；推动集成密码创新和融合应用，有效落实《中华人民共和国密码法》及相关合规性建设在政务系统的落地，为政务系统塑造完善的密码管理与服务体系，为政务云密码安全提供坚实的基础支撑。

六、适用行业：

全行业

七、联系人姓名及职位

姓名：陈宇

职位：资深产品专家

联系方式：18600336941

八、CEO/创始人/总裁/副总裁/联合创始人等对行业发展和甲方的寄语：

各行各业的网络安全建设一直都在持续投入，安全防护不断加固，但各类安全事

件仍旧时有发生，安全体验也有颇多抱怨，究其原因，安全建设不应该只是成本中心，更应该成为业务需求的驱动中心。新华三认为安全应该更主动一些，一是坚持主动安全防护理念，将安全作为顶层设计去考虑。二是以技术和运营作为两大抓手，通过技术框架打造防御体系，以安全服务提升安全体验，真正实现同步建设与运营。三是夯实三个关键技术：通过情报加持威胁治理，基于场景构建 AI 模型并以云边协同构建起立体的安全体系，让防御更快、更准、更智能。

——新华三集团副总裁、新华三信息安全技术有限公司总裁 孙松儿

信安世纪

一、公司名称：

北京信安世纪科技股份有限公司

二、公司 logo：

三、商用密码产品名称：

信安 NetEDS 数据加解密服务系统

信安 NetIAG 安全认证网关

四、产品特点及优势：

信安 NetEDS 数据加解密服务系统：

特点：

信安 NetEDS 数据加解密服务系统是一款基于商用密码技术实现的高性能数据

安全产品。该产品能够对敏感数据、重要信息等进行加密保护，在有效降低因数据泄露带来的安全风险的同时，帮助用户切实履行 《数据安全法》、《个人信息保护法》等法律法规要求的数据保护义务。主要核心功能包括：

全生命周期密钥管理

密钥管理服务可提供基于 KMIP 协议或 REST 风格专有协议实现密钥全生命周期管理，采用三级密钥体系及硬件加密技术，保障密钥的机密性。拥有完备的密钥备份、归档、恢复机制，充分保障密钥的完整性与可用性。

通用加解密服务

提供 REST 风格的 HTTP API 接口，通过数据的加解密、签名验签、数字信封、数字摘要等功能，保障信息在传输与存储过程中的完整性、机密性、不可否认性和真实性。

切面加密服务

基于字段级的数据库加解密能力 ,提供对数据的脱敏处理以及对存量数据的加密服务，并且支持自定义加密策略，实现无需改变格式的加密。

访问控制

支持 RBAC、ABAC 鉴权的访问控制机制。通过授权应用 ID 和授权密钥等信息，完成应用访问安全认证，防止非法访问。同时，支持运维管理的三权分立，明确管理职责，为系统提供更安全的管理体系。

Web 管理界面

页面简洁、功能齐全，提供密钥管理、切面加密管理、应用管理、系统设置、用户管理、日志管理等功能，方便用户灵活配置策略，对用户操作提供全方位的保障，帮助用户进行高效管理。

优势：

- **多场景**

适用于统一密钥管理、多云密钥管理、数据库加密、存储加密等多种应用场景，满足数据安全和个人信息保护的需求。

- **强安全**

支持 TLCP 协议（国密 SSL）实现 API 通讯加密，满足 GM/T 0028-2014《密码模块安全技术要求》第二级安全要求。

- **高性能**

支持千万级密钥容量，可达到万兆级加解密性能，并且支持万级并发处理能力，保障系统高效运行。

信安 NetIAG 安全认证网关：

特点：

信安 NetIAG 安全认证网关是一款融合零信任特性的应用安全产品，产品基于商用密码技术实现，有效解决用户使用应用系统时设计的身份验证、数据传输加密、

权限控制等安全性难题，在大大提高企业应用系统安全性的同时，最大程度简化接入过程，提升业务效率。

优势：

- **自适应身份鉴别，提升用户身份安全性**

根据实时的终端安全等级评估结果，为高风险的接入请求添加第二安全要素的身份认证，实现自适应身份鉴别，保障接入主体的身份安全性。

- **国密级传输加密，提高数据传输安全性**

产品采用 TLCP 国家标准协议（即国密 SSL 协议），提供基于 SM2、SM3、SM4 商用密码算法实现的通信加密能力，充分保障数据传输过程中的机密性和完整性。”

- **网络隐身功能，有效隐藏企业数字资产**

通过 SPA 网络隐身技术，使得企业应用只对合法主体可见，不为潜在攻击者提供任何端口的监听信息，有效防范恶意攻击，为企业应用和服务披上了“隐身衣”。

- **动态访问控制，实现持续安全防护**

基于角色的访问控制策略引擎，可以为不同的用户角色定制授予不同的应用权限，同时在用户访问期间通过对其安全状态进行持续评估，实现动态地、精细化的安全防护。

五、成功案例：

某银行零信任安全解决方案:

安全需求：

随着内外部网络环境的变化，企业面临的安全威胁愈演愈烈，零信任作为一种以资源保护为核心的网络安全新兴理念，正逐渐被越来越多的企业接受，零信任也迎来了体系化、集成化新时代。

解决方案：

信安世纪零信任解决方案基于 SDP 软件定义边界技术、IAM 身份识别与访问管理技术等，并结合了商用密码技术，通过网络隐身、以身份为核心、可信业务访问、动态访问控制、多源信任评估等核心能力帮助企业解决传统的网络安全边界理念与防护手段不足的问题，构建以身份为边界的零信任安全模式，营造安全、可信的网络环境。

方案优势：

- **以商用密码技术为基础，实现通信双方的可信鉴别和安全加密通讯**

信安世纪零信任解决方案基于等级保护相关要求策划完成，符合合规、正确、有效的密评标准。在认证方面，方案采用基于国密算法的证书和动态口令，支持国密 SM2、SM3、SM4 等加密算法，有效保障数据的安全性；在通信方面，方案采用 TLCP 协议进行隧道加密，保障流量在安全的加密通道上传输，实现数据完整性保护；在密钥管理方面，采用协同签名技术做密钥分割，充分保证密钥的安

全性，大大降低了私钥泄露的风险，提升整体的安全防护能力。

- **以身份管理技术为核心，实现持续的身份认证和动态访问控制**

方案支持零信任自适应身份认证，可根据多因素动态调整身份认证策略。通过零信任安全代理客户端来获取终端安全状态，将终端环境感知与风险信息上报至零信任安全认证网关；零信任安全认证网关将信息转发给策略中心，策略中心根据上报的日志，对终端环境和风险信息进行综合建模，实现持续的信任评估，并将评估结果推送到动态授权模块，为用户提供动态的、近乎实时的、自动的权限调整，做到整体的安全闭环。

- **以安全网关技术为支撑，实现大规模、复杂场景的灵活部署和应用交付**

为了满足灵活部署需求，方案提供产品软硬件的不同部署方式，支持在虚拟平台和公有云平台上通过虚拟化软件的方式部署。同时，网关单台硬件设备支持超高吞吐量，满足大流量的客户需求；支持用户数最高可达几十万量级，满足海量接入的需求。此外，在保证性能和安全的前提下，还集成了硬件 SSL 加速、连接复用、HTTP 压缩、集群等功能，具有灵活的可扩展性。即使在出现故障时，信安世纪 N+1 集群技术也可以确保终端用户的体验和访问不受影响。

- **优秀的 SPA 网络隐身能力，隐藏企业数据资产、最小化攻击面**

方案支持 SPA 单包授权机制，在接入企业网络之前，客户端会先将必要信息集成在单个数据包内，携带数据包至信安零信任系统，信安零信任系统进行身份校验，只有验证通过后才能进行认证授权，且不会开放额外端口；而未携带 SPA 包的客户端，在访问零信任系统时，则不被允许通过。通过此种方式，可以有效

隐藏企业数据资产，从而降低攻击风险。

- **以企业现有安全架构为依托，实现客户化、异构化的零信任安全架构**

信安世纪零信任解决方案具备极强的适应能力，可以集成企业已有的安全产品，与现有的网络安全管理融合形成联动，而无需改动现有的软硬件设备及网络环境，实现零信任安全能力持续增强。方案支持跨平台 API 以及开放的接口标准和规范，实现对多种应用系统的集成，保障整体网络架构的稳定运行。

- **以丰富的登录认证场景为优势，带来无感、友好、一站式的访问体验**

方案支持 B/S、C/S、远程 RDP 等丰富的单点登录场景，用户只需通过一次强身份认证，即可无感知访问授权范围内的系统应用。支持人脸识别、指纹认证、国密证书等十几种登录方式以及多种操作系统、浏览器、移动设备的远程接入，满足随时随地移动办公需求。

高性能数据加密保护-某客户项目:

业务场景：

某客户要求部署符合密码相关国家、行业标准要求的密钥管理与数据加解密服务系统，对其 16 个业务系统进行数据加密保护，要求不对其 16 个业务系统进行改造，但需提供隐私数据脱敏能力。

安全需求：

- 针对客户 16 个业务系统提供高性能数据安全防护，对业务系统中重要数据进行存储机密性、完整性保护，实现重要数据防窃取和防篡改保护。
- 同时提供方便快捷的密钥全生命周期管理服务，将 16 个业务系统中的密钥进行统一管理，便于运维。
- 对其隐私数据，根据不同敏感数据采用不同脱敏策略，实现自定义脱敏能力。

解决方案：

- 保证该客户 16 个业务系统相应隐私数据的加密保护，满足安全合规要求。
- 通过切面数据加密方式，确保业务代码无改造；通过解析 SQL 方式将隐私数据加密存储于数据库中，保障数据的机密性、完整性。
- 通过管理平台对 16 个业务系统中的密钥进行统一的全生命周期管理，同时支持密钥自定义轮转，节省运维人员工作量，提高密钥管理安全性。
- 提供基于身份授权的数据脱敏服务，可针对手机号、身份证号、银行卡号等隐私信息进行转换、修改或者遮盖的脱敏处理操作，实现授权用户正常查看数据信息，部分授权用户查看脱敏后数据信息，未授权用户不能查看数据信息的用户最小化授权，防范隐私信息泄露风险。

六、适用行业：

金融、政府、企业、运营商、交通、社保等行业

七、联系人姓名及职位

姓名：陈晓萍

职位：市场经理

联系方式：01068025518

八、CEO/创始人/总裁/副总裁/联合创始人等对行业发展和甲方的寄语：

随着云计算、大数据、移动互联、5G、工业互联网等新兴技术的蓬勃发展和成熟应用，网络安全已经成为实现数据资产安全应用、加快数字化发展、建设数字中国的核心基础和重要保障，这给信息安全与商用密码市场带来了更多发展机遇。

信安世纪作为科技创新型信息安全企业，将坚持以市场需求为导向，重点加大行业应用开发，提升公司安全产品的高质量应用；并在技术研发上坚持创新驱动发展，不断夯实技术基础，加强基础性、通用性、前瞻性安全技术的研究，加快关键核心技术攻关，朝着“更深、更宽、更广”的方向持续布局，以己之力推动信息安全产业链的高速发展。

——北京信安世纪科技股份有限公司 董事长 李伟

赢达信

一、公司名称：

天津赢达信科技有限公司

二、公司 logo：

三、商用密码产品名称：

智能密码钥匙、国密安全浏览器、手机盾认证系统、数据库加密管理系统

四、产品特点及优势：

特点：国密二级产品安全性高、原有应用少改或无须改造即可进行商用密码应用改造。

优势：接口设计灵活，与其他厂商产品能够快速联调完成商用密码应用改造。

五、成功案例：

金融行业中网银客户端与 SSL 安全网关集成密码应用改造，提升客户端及通道的机密性和完整性保护，目前已广泛应用于 30 多家中小型银行证券等机构中。

国密安全浏览器与客户端重点客户案例：

民生银行、光大银行、浦发银行、平安银行等网银客户端

山东城商行合作联盟、顺德农商银行等网银客户端

中国结算、郑州商品交易所、中国证券业协会等安全浏览器

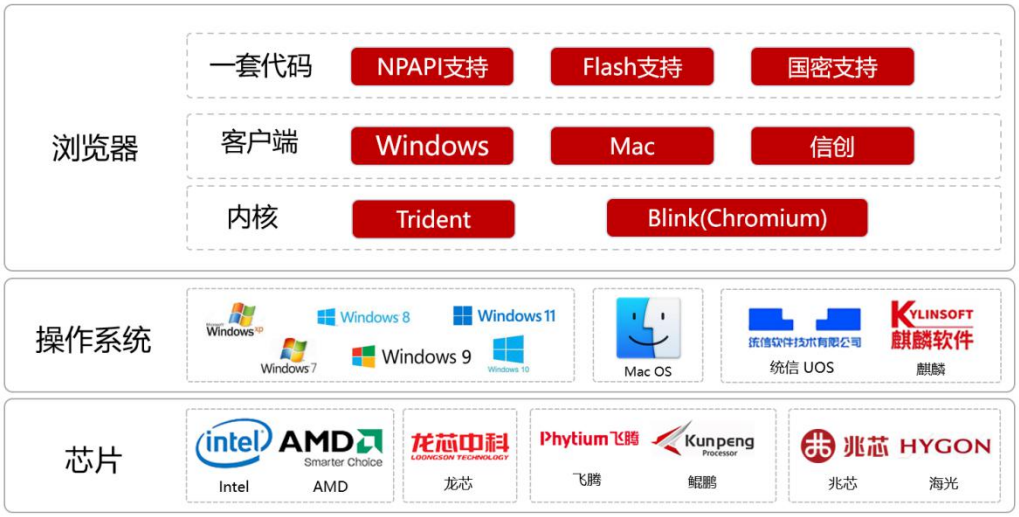
数据库管理系统实现数据库的透明加密，在密评密改项目中属于必须建设事项。与采用密码机加密数据的方式对比，无需应用修改业务系统，可实现快速上线。适用于政企、金融等高安全需求的行业等。

数据库加密管理系统重点客户案例：

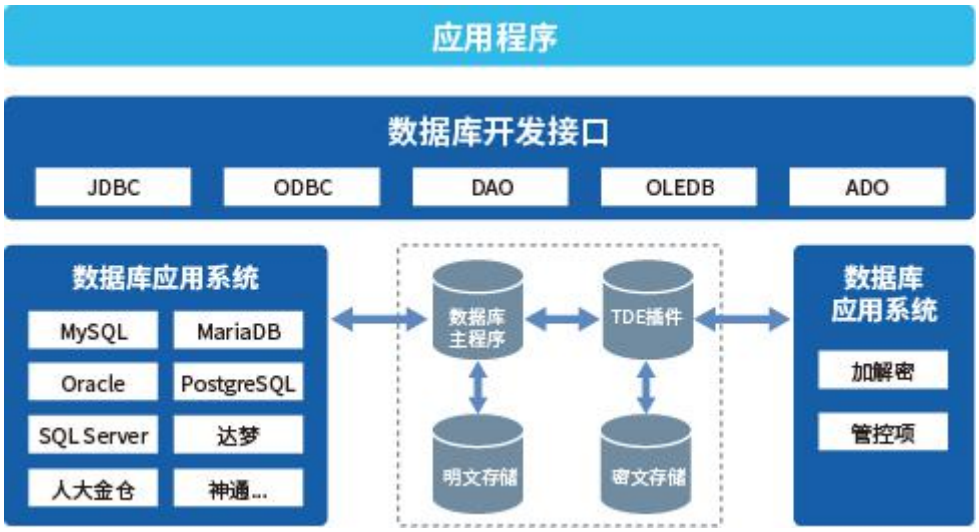
四川省眉山市住建局

宁夏公共安全视频监控密码应用安装改造项目

云南省电信号百分公司业务系统密改项目



浏览器技术架构图



数据库加密管理系统技术架构图

金融网银客户端重点客户名单

六、适用行业：

政务、金融、公安、能源、交通、教育和医疗等

七、联系人姓名及职位

姓名：彭竹

职位：产品总监

联系方式：18601092821（微信）

八、CEO/创始人/总裁/副总裁/联合创始人等对行业发展和甲方的寄语：

目前行业由于密码法的颁布进入了快速发展期，生态产业界的同仁们更加紧密的协同和合作起来一起为甲方提供更快速更优质的整体密码服务解决方案。赢达信科技专注于终端安全硬件、安全浏览器的研制及手机盾认证系统与数据库加密管理系统等密码应用系统的各类产品、系统和服务的开发，提供针对政企、金融及其他行业应用的采用密码技术的安全解决方案。期望与业界同仁一起开创密码行业的新时代。

——赢达信总经理 李宝盛

云上密码

一、公司名称：

云上（江西）密码服务科技有限公司

二、公司 logo：

三、商用密码产品名称：

全鉴®密码服务平台

四、产品特点及优势：

特点：

全鉴®密码服务平台是云上（江西）密码服务科技有限公司自主研发的集约化密码服务平台，可为“通用+信创”环境下的信息系统提供统一密码服务，保障业务系统在身份识别、安全隔离、信息加密、完整性保护、抗抵赖性等方面的密码防护，实现各级信息系统密码应用的合规性、正确性和有效性，符合 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》等要求。

优势：

1.集约化

平台建立了统一的密码资源池，以跨平台中间件的形式对外提供统一密码服务接口，极大避免密码软硬件重复投入；同时，通过集约化的平台部署，可兼容传统密码应用方式遗留的密码硬件资源，充分“利旧”，提高资源利用率。

2.国产化

平台以具有国推商密产品认证证书的服务器密码机、签名验签服务器、SSL VPN等密码软硬件设备为基础，同时适配“龙芯+银河麒麟”“飞腾+中标麒麟”等信创环境，支持在“混合云”环境（通用环境+信创环境）中部署应用。

3.模板化

平台采用了简洁、方便的密码软硬件架构体系，在组织保障、制度规范、项目管理、密码建设等方面总结了经验，形成了云模式下的密码服务体系建设模型，为地市政务云密码服务体系建设提供了可借鉴、可复制的模型样本。

五、成功案例：

全鉴®密码服务平台作为江西省第一个通过密评的信息系统，自运行以来成效显著，已经在省纪委、省公安厅、省水利厅、省信息中心及南昌市、景德镇市、宜春市等地部署实施，已为省委政法委的“跨部门大数据办案平台”、省财政厅的“财政身份认证与授权管理系统”、省粮食局的“粮食数据管理中心系统”、省信息中心的“赣政通”协同办公平台等近百个业务信息系统提供了密码应用服务

保障，协助超 50 个重要信息系统通过密评。

应用案例：“赣政通”协同办公平台

客户需求：作为全省政务工作人员协同办公的“总入口、主平台”，该平台依法应使用商用密码并开展密评。

使用效果：云上密码公司已在省政务云上部署好了全鉴密码服务平台。该协同办公平台可方便快捷调用密码平台提供的弹性合规密码服务，更好更快通过密评。

六、适用行业：

可广泛应用于金融、税务、教育、电信、电子政务、电子商务等重要领域。

七、联系人姓名及职位

姓名：邹紫凯

职位：策划

联系方式：18566070723

八、CEO/创始人/总裁/副总裁/联合创始人等对行业发展和甲方的寄语：

不忘初心，守护命门。以拳拳之真心报国家之信任，以密码之进步筑国家之坚盾。

——云上密码总经理 姜林海