



江南科友—行业敏感数据云服务平台解决方案

契合各行业信息安全保密需要，解决企业最核心数据安全关键问题，提供最佳密码应用支持。



江南科友具有独立的商业密码技术知识产权，具有一系列完整的涉密设备和软件产品的生产和销售资质，及涉密项目集成和服务资质，科友的所有软硬件产品都具有国密局认证资质产品。

江南科友一直以来是国内密码技术商业应用的领先者，我们通过提供密码技术产品及服务，帮助各行业的客户保护最核心数据的安全。

95.9%的手机用户
遇到过手机信息安全事件

省公安机关每月发现**10**款移动APP
，存在窃取用户信息等安全问题

47.3%的用户
因为各类安全事件造成过损失

移动金融APP从2014~2016年，发
生安全事故**1000**多起

恶意窃取数据

恶意行为的挑战，非法人员可能通过利用软件错误与恶意行动来获取敏感数据

数据安全 责任明确

云服务商、企业、个人对数据保护要求和责任的明确

端到端 数据安全保护

做到端到端的安全，在薄弱环节的安全控制缺失导致数据泄露、破坏

安全 透明度

安全风险分析和通知机制，数据保护安全的透明性，提升用户的满意度

全服务 周期保护

确保在服务终止等情况下，用户敏感数据得到充分的保护

灵活性、可用性与安全的平衡

在数据的灵活访问和使用情况下，数据的保密安全的实现

行业敏感数据云服务平台解决方案架构



移动手机端

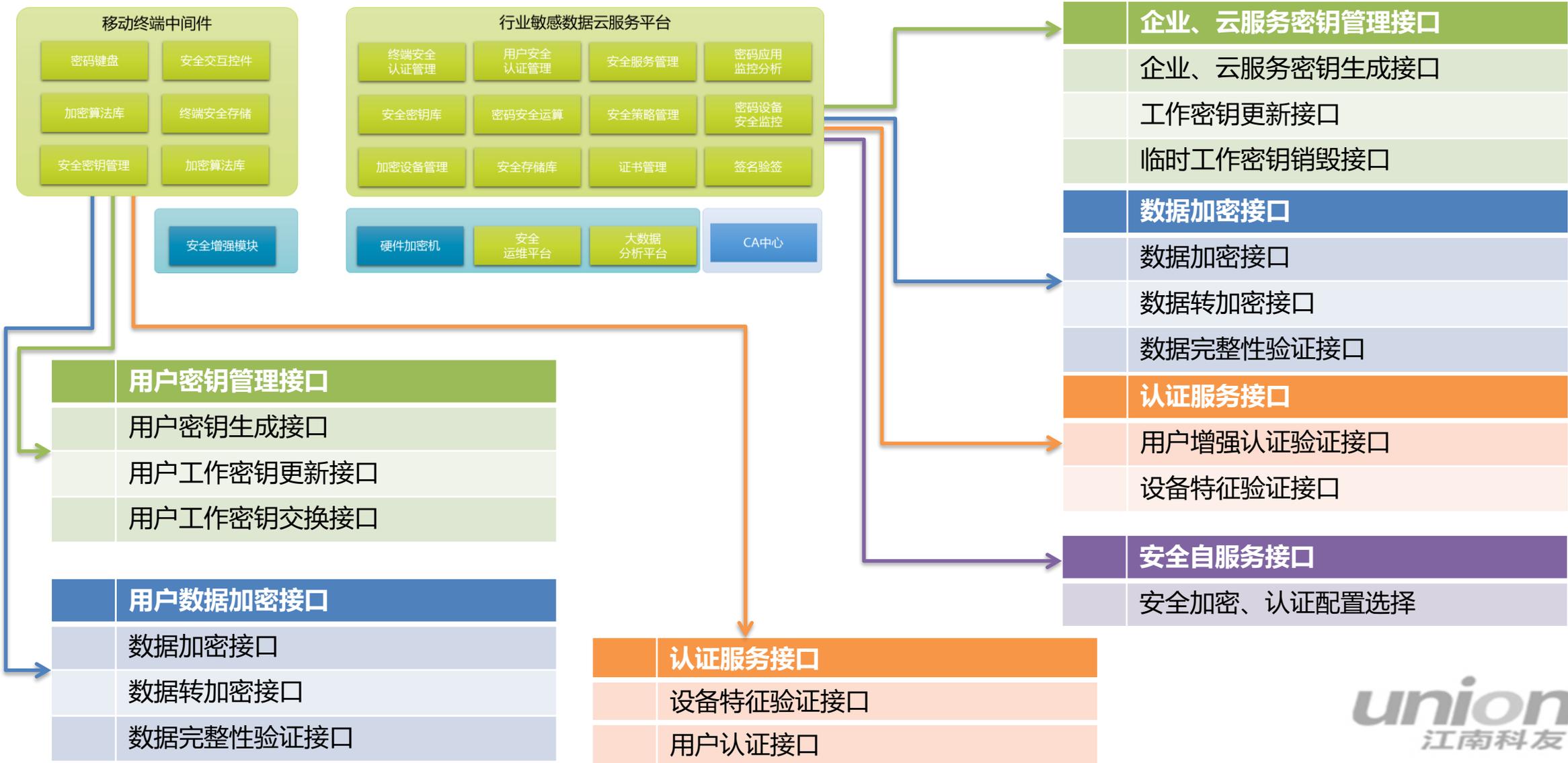


云服务端

基于行业应用特点设计密钥体系，提供高级别数据安全保护



提供开放中间件接口与服务端接口便于行业应用对接



医疗行业数据应用安全示例



目前互联网医疗应用已经超过2000种；
几乎没有任何互联网医疗应用考虑过用户的隐私及数据安全；
没有安全性可言的环境不利于医疗大数据的发展。

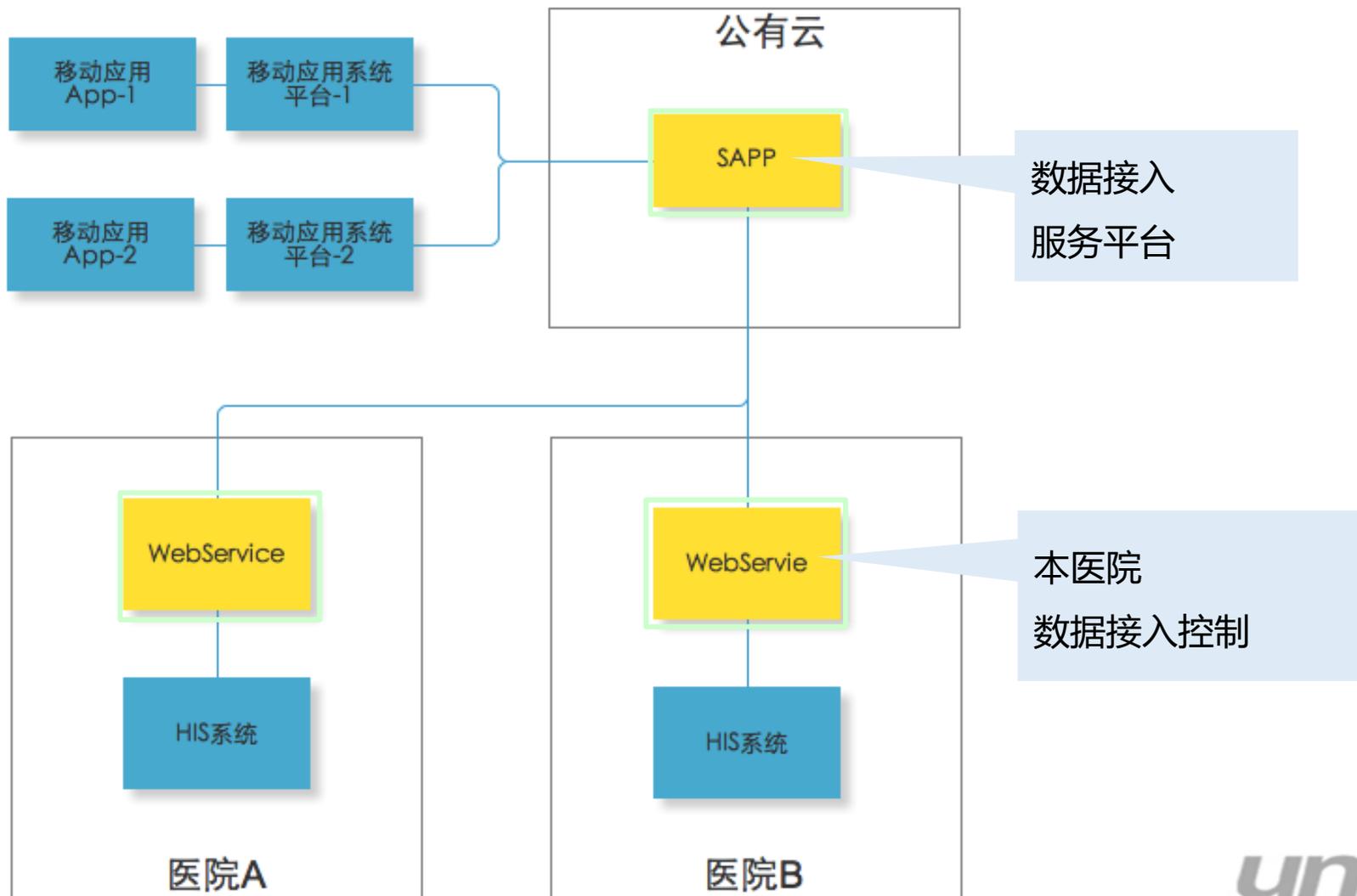
要求	说明
防止数据滥用	医院等机构作为数据源所有者，如何合理的控制数据的访问权限，敏感数据开放给服务商，医院失去信息控制权，信息存在 被滥用的风险
数据授权控制	只有用户本人才能读取敏感信息，其他人员无法解析数据，服务商也无法截获敏感数据，实现了 精确的数据授权控制
端到端数据保护	无论是在手机终端、应用服务商、数据服务平台，数据都能得到安全保护，除了数据所有者、授权的数据使用者，没有其他实体能够访问敏感数据，实现 端到端安全保护
数据安全警示	当有异常安全事件发生时，如发生用户异常登陆、不正常的敏感数据操作等，及时得到 安全风险警示
数据保护规范化	促进行业移动应用 敏感数据保护的规范化和标准化 ，改变医疗行业敏感数据使用混乱的局面

医疗行业移动数据当前业务模式



业务场景

- 1、预约缴费
- 2、查询记录
- 3、处方取药
- 4、医嘱随访
- 5、病历推送
- 6、保险理赔
-



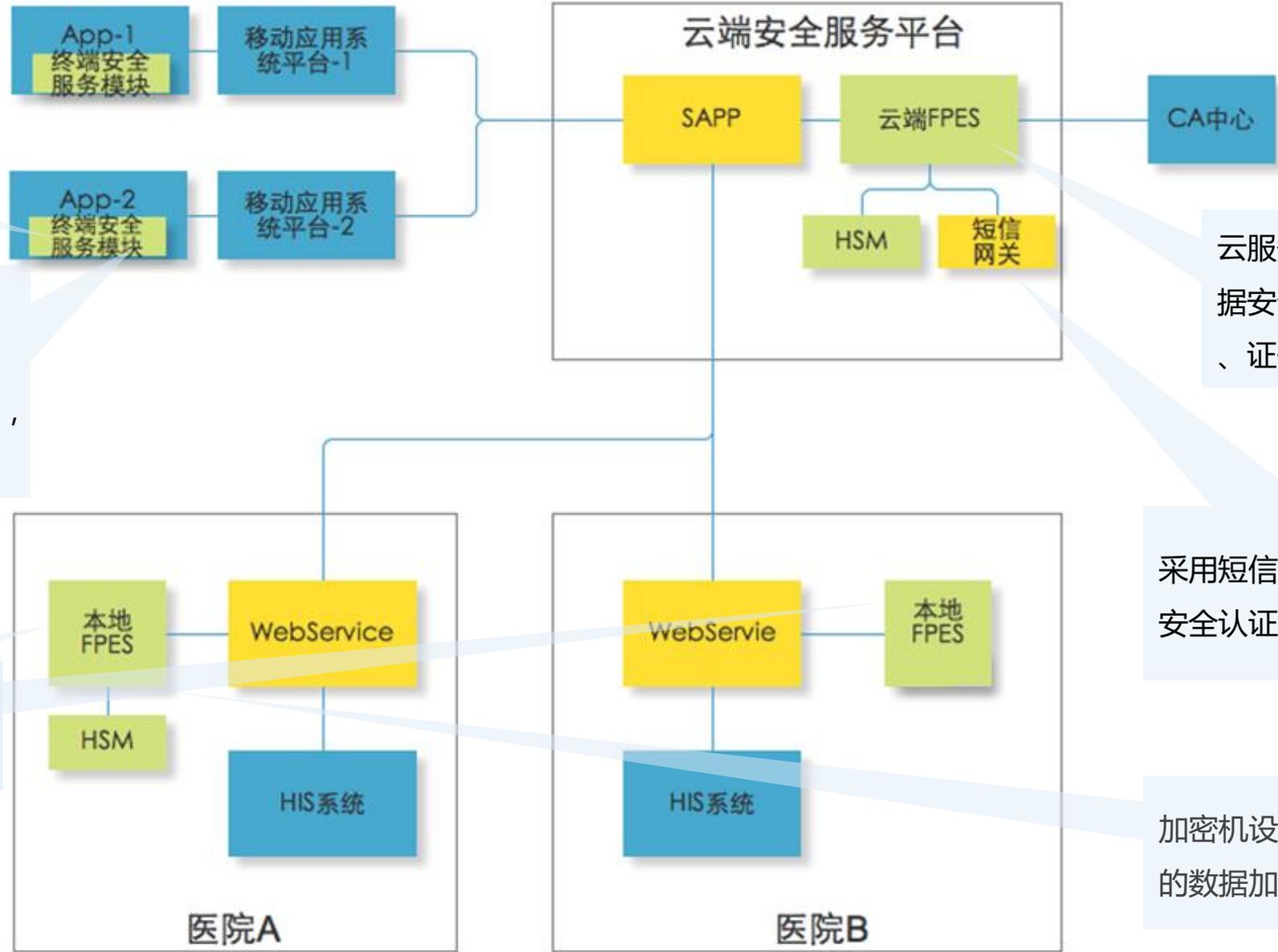
集成敏感数据云安全服务平台，提升医疗数据安全保护水平



敏感数据在移动端加密存储，保障数据被非法窃取和破坏安全

APP调用终端安全模块，实现数据受控访问；同时由终端安全模块提供安全的人机交互，避免被截取滥用。

医院端对敏感数据实施安全控制



云服务平台提供统一数据安全认证、风险警示、证书管理等服务

采用短信验证码，增强用户安全认证

加密机设备提供高效、高安全的数据加密



■ 端到端敏感数据的安全控制

- 1、用户只能查看本人敏感数据
- 2、数据源端通过安全策略控制加密密钥及加密过程
- 3、可实现对不同级别的用户、设备的敏感信息访问控制机制

■ 多层次安全验证

- 1、云端用户状态动态管理
- 2、基于PKI的互信机制
- 3、短信验证码增强用户认证
- 4、支持增强的安全认证如动态令牌、蓝牙令牌等

■ 系统部署及使用灵活

- 1、采用云服务+移动计算方式实现医疗敏感数据安全保护
- 2、支持标准的SDK应用集成方式，统一的业务及安全服务调用入口，广泛支持多种类型移动智能终端
- 3、云服务平台化，可与不同的应用服务商、不同的数据源企业组织进行对接
- 4、数据源端可采用HSM硬件加密或软加密等多种灵活部署方式，满足业务灵活需求
- 5、可与公共CA系统对接，支持APP端、政府网站、医院本地等的线上、线下用户证书申请
- 6、根据各类型数据源机构的数据安全保护要求来灵活配置和部署，不增加一般用户使用的复杂度

科友为该银行设计实施机密云项目，实现用户数据资产的“极度安全和极度隐秘”



项目目标

将银行传统的保险箱业务与移动互联数据服务结合起来，以“极度安全，极度隐秘”的理念打造数字资产保险箱业务，在保护客户隐私的同时为各类账号、密码以及各种文件提供操作便捷的管理空间。

项目方案

让用户掌控主密码的核心设计理念，主密码是一切可控可信的根源，应用密钥由主密码随机生成加密因子，杜绝了黑客和服务商自身的数据窃取风险，即使是银行内部的工作人员也无法看到用户的主密码及存储内容

实现短信验证、手机指纹、一机一密等安全认证方式，这种组合拳式的安全认证构成移动应用所独有的安全体系。

行业敏感数据云服务平台解决方案优势



适应不同行业敏感数据移动应用安全保护需要，提供集中统一的基于云的服务平台以及规范、便捷的服务接口，能与各种行业类型数据应用进行集成对接，提供高安全、可信赖的数据保护服务



商用密码技术领域具有专业坚实的理论和运用实践经验，具有专业的研发团队和技术服务团队



经过国密局深度安审，可以信赖的性能卓越的产品符合国家信息安全法规和保密要求



具有跨行业合作经验，提供根据不同行业特色，提供切合实际需求的全加密安全解决方案

谢谢！