2023

智安网络

ZHIAN NETWORK

云密-统一密码服务平台

技术白皮书

AQ-SC-080 V1.0

市场指南

深圳市智安网络有限公司

www.zhiannet.com

目录

1 概述

在当今数字化时代，互联网的普及和信息技术的迅猛发展，网络攻击和数据泄露的风险日益增加，黑客、恶意软件和网络犯罪活动对企业和个人的隐私、财产和声誉造成了严重威胁。国内网络空间安全形势也存在核心技术受制于人、信息产品存在巨大安全隐患、关键信息基础设施安全防护能力薄弱等问题。

随着《中华人民共和国密码法》颁布和新修订的《商用密码管理条例》的出台，商用密码在维护国家主权、安全和发展利益以及保障网络和信息安全方面的作用越来越凸显，网络建设合规性日益重要。商用密码在身份鉴别、数据加密、可信认证等方面发挥着重要的作用。

2 产品描述

智安云密·统一密码服务平台是集密码资源统一管理调度、密码服务统一管控、密钥集中管理于一体的服务管理平台。平台以虚拟化、可视化、一体化的服务理念为应用提供按需分配、弹性伸缩、灵活拓展的密码应用新模式，可广泛应用于电子政务、金融业务、医疗健康、能源电力、教育、交通等多种应用场景。

智安云密·统一密码服务平台采用密码运算单元自适应技术，实现密码资源的弹性拓展、弹性自愈，灵活调度应用各种复杂场景；采用密钥安全分发技术，保证密钥全流程流转安全，构建密钥安全托管模式；系统软硬件构成包含服务器、用户终端、网络设备、存储、安全防护设备、密码设备等硬件资源和操作系统、数据库、应用中间件等软件设备资源。

3 产品标准

智安云密·统一密码服务平台是深圳市智安网络有限公司研发的集典型密码服务、通用密码服务、密钥管理服务于一体的密码产品，遵循以下密码行业标准：

《密码模块安全技术要求》(GM/T 0028-2014)

《密码应用标识规范》(GM/T 0006-2012)

《密码设备应用接口规范》(GM/T 0018-2012)

《通用密码服务接口规范》(GM/T 0019-2012)

《时间戳接口规范》(GM/T 0033-2014)

《SM2 椭圆曲线公钥密码算法》(GM/T 0003-2012)

《SM2 密码算法使用规范》(GM/T 0009-2012)

《SM2 密码算法加密签名消息语法规范》(GM/T 0010-2012)

《密码设备管理 设备管理技术规范》（GM/T 0050-2016）

《密码设备管理 对称密钥管理技术规范》（GM/T 0051-2016）

《公钥密码应用技术体系框架规范》（GM/T 0094-2021）

《云服务器密码机管理接口规范》（GM/T 0088-2020）

4 产品特点

集中管控，服务中台化：集约化建设密码资源池，不需要再重复密码软硬件设施建设，提高资源利用率，显著降低了建设成本、管理运维成本，运用密码技术中台实现服务的标准化、统一化封装，提供高度封装的密码服务接口，为业务应用提供灵活易用、易于集成、透明高效的支撑服务接口，实现节省密码学习、流程梳理、底层调用等时间成本，降低应用

开发适配难度。

灵活部署，管服分离：以密码云化部署解决应用对密码的服务需求，采用微服务架构，实现服务重用，服务进化，组件式管理，支持热部署，中台服务支持双活、集群部署，确保中台服务的高可用性。密码服务中台、密码服务管理平台、密钥中心可以灵活部署，实现密码管理与密码服务有效分离，完善运行机制。

安全兼容，服务可视化：支持麒麟、统信国产操作系统以及 Linux、Windows 等操作系统，支持动态增加底层的密码设备，支持对密码设备进行分组管理、负载均衡，提供全方位密码应用、运行和状态可视化视图，实现密码运维可见、可控、可管，有效保障网络安全。

5 产品功能

智安云密·统一密码服务平台产品技术架构如下图 5-1 所示：

图 5-1 技术架构图

基础设施层：分为云基础设施和密码基础设施两部分，密码基础设施

以密码设备构建的密码资源池，基于虚拟化技术的密码资源池具备动态扩容、故障漂移等能力；云基础设施为某私有云提供的虚拟化计算资源、虚拟化存储资源、虚拟化网络资源等。

平台能力层：依托密码基础设施和云基础设施提供了合规、安全的密码能力；能够提供高可靠、高可用的密码服务，具备动态扩容、灰度升级等特性。

平台管理层：平台运维管理是密码服务平台的运维平面，能够对平台的资源、系统配置、人员进行管理和维护，保证平台的可靠运行，为管理用户业务的密码支撑提供可靠性、可用性、可维护性支撑。用户平台是租用户对自身密码功能的管理，以用户应用为中心，为不同用户应用提供密码资源、密码功能支持。

接口层：用户可开通相应的密码服务获取密码服务接口的调用权限，支持 RESTful 接口。

5.1 设备管理功能

密码服务平台使用密码资源池的概念设备进行集中管理；平台支持管理虚拟化的云密码机与传统的密码设备；密码服务平台实现了对密码资源的统一调度和分配。密码设备是密钥保护的基础，也是密码运算的主体，平台通过集中的设备管理实现密钥保护的安全性及密码资源的优化调度。

5.2 密码基础运算服务

密码服务平台使用密码资源池的概念设备进行集中管理；平台支持管理虚拟化的云密码机与传统的密码设备；密码服务平台实现了对密码资源的统一调度和分配。密码设备是密钥保护的基础，也是密码运算的主体，平台

通过集中的设备管理实现密钥保护的安全性及密码资源的优化调度。

● 支持 SM2、SM9 等国密标准非对称算法；RSA、DSA、ECDSA 等国际标准非对称算法。

● 支持 SM1、SM4、SM7 等国密标准对称算法；DES/3DES、AES 等国际标准对称算法。

● 支持 SM3、SHA1/SHA2 等杂凑算法。

● 支持双 WNG8 物理随机源生成真随机数。

5.3 密钥管理服务

密钥管理服务支持包括对称密钥、非对称密钥、数字证书和秘密数据等多种加密对象的统一管理。通过对加密对象的统一管理，可简化密钥管理操作，使加密变得更易于配置和管理， 减少了密钥管理系统的维护成本，满足企业多应用多业务场景的密钥管理需求。

密钥结构采用“系统保护密钥-用户密钥（内部密钥对或 KEK）-会话密钥”的三层密钥保护结构，保证关键密钥在任何时候不以明文形式出现在设备外，密钥备份文件受备份密钥加密保护。

1) 加密对象全生命周期管理

提供对称密钥、非对称密钥、数字证书等加密对象的状态管理和属性管理。完成对加密对象的生成、存储、激活、分发、更新、注销和销毁等全生命周期管理操作及加密属性的取、添加、修改和删除等操作。

2) 安全密钥生成

密钥管理系统密钥采用由国家密码管理局批准使用的物理噪声源产生器芯片生成的随机数，密钥生成后由 HSM 模块中的系统保护密钥加密后存

储。

3) 多种算法密钥管理

支持 SM4、AES、3DES 等对称算法密钥的生成与管理；

支持 SM2、RSA、ECDSA 等非对称算法密钥的生成与管理；

支持 HMAC-SM3、HMAC-SHA1 等密钥的生成与管理。

4) 密钥安全下发

客户端业务系统密钥获取操作支持 SSL 数字证书、密钥用户名和口令等多种认证及加密方式，几种方式可灵活组合配置。保证敏感信息在经过网络传输过程中的安全性，避免接口通信信息泄露、中间人攻击、重放攻击等可能性。

5.4 SSL VPN 服务

SSL VPN 加密服务支持多种安全合规的算法协商套件并对低版本的客户端提供了弱算法兼容支持，符合等保、密评等对密码设备、密钥管理、国密运算的要求。采用优化的异步 I/O、Cache 和 Pool 机制，通过 SSL 卸载、连接复用、HTTP 压缩、WEB 缓存、会话保持机制等方式将复杂的 SSL 加解密压力转移到安全网关，并使用专业的、灵活的调度算法提供四层到七层的 WEB/TCP/UDP 服务的负载均衡功能。

1) 动态证书认证

可处理单双向 SSL 连接，并且可同时处理多种类型和多个应用的 SSL 加解密处理，同时支持国际标准算法及国密 SM 系列算法；支 OCSP 自动查询、LDAP、手工上传等多种动态认证方式；支持多证书来源、多站点证书认证。

2) 应用服务支持

支持不同类型服务的 SSL 代理，支持四层 WEB、TCP、UDP 协议的服务调度代理，支持应用服务的 URL 映射、协议头转发、细粒度访问控制和基于证书的用户黑白名单配置等。

3) SSL 卸载

服务具有高性能的 SSL 处理能力，不但能够实现端到端的 SSL 加密，同时支持全面的加密算法配置，并具备完整的证书管理特性。

4) 连接复用

服务将众多客户端连接请求捆绑后，复用相对较少的服务器 TCP 连接，而不用通过一对一的方式把每一个用户的 HTTP/TCP 分配到服务器。

5) 会话保持机制

服务的会话保持技术，可以为访问用户选择曾连接上的特定服务器，实现无缝地处理用户请求；另一方面可以减少新建连接的数量，有助于减小负载均衡设备的系统开销。

6) 负载均衡

服务支持四层到七层的 WEB/TCP/UDP 服务的负载均衡配置，提供多种负载均衡算法将所有流量均衡的分配到各个服务器，不仅充分利用所有的服务器资源，而且各个服务器均衡的承担流量处理任务，从而有效地避免服务器处理任务“不平衡”现象的发生。

5.4 时间戳服务

时间戳服务完全符合《信息安全技术 公钥基础设施 时间戳规范》（GB/T 20520-2006）、《时间戳接口规范》（GM/T 0033-2014）。时间戳服务

使用国家密码管理局审批的密码算法和硬件加密设备。底层采用符合《GM/T0028-2014 密码模块安全技术要求》安全二级要求的密码设备，产品安全性得到国家认可。时间戳服务符合国家标准，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。时间戳服务支持 SM3 摘要算法，支持 SM2 密码算法时间戳签发。

时间戳服务从国家权威标准时间发布机构获取标准时间，综合使用公钥加密技术、数字证书和数据摘要技术，为用户的信息数据签发可信、权威的时间戳。

5.4 签名验签服务

签名验签服务能够对各类电子信息数据、电子文档等提供基于数字证书的数字签名服务，并可验证签名数据的真实性和有效性;支持不同 CA 的用户证书验证，提供基于根 CA/CRL/OCSP 等多种方式的证书有效性验证。满足用户在网络行为中真实性、不可否认性、完整性、机密性等需求。

6 产品部署

云密码机部署拓扑图如 6-1 所示：

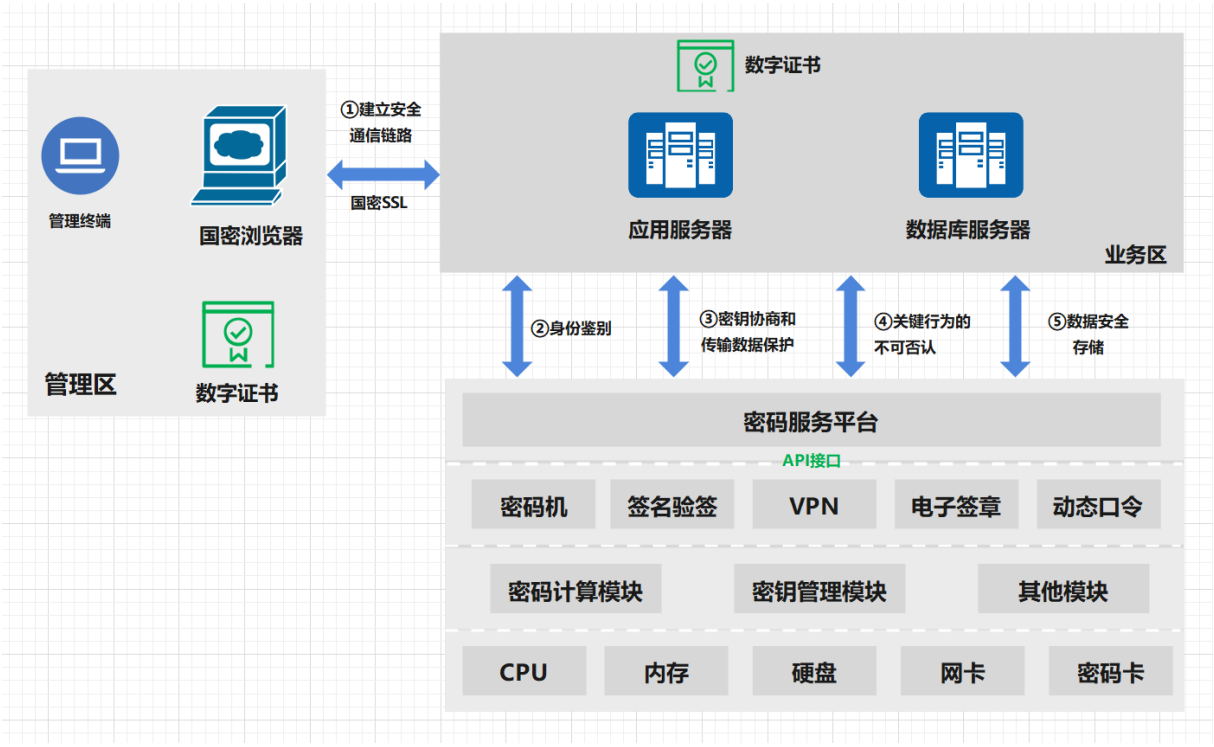

图 6-1 产品部署

密码设备资源池部署于云计算资源池中，主要密码设备包含云服务器密码机、签名验签服务器、时间戳服务器、SSL VPN 等基础设施，为业务系统提供密码服务支撑。

智安云综合防御平台密码云部署在业务区，与业务系统网络可达，向下管理调度密码服务计算资源，向上层提供密码基础服务、密码业务服务等。

7 应用场景

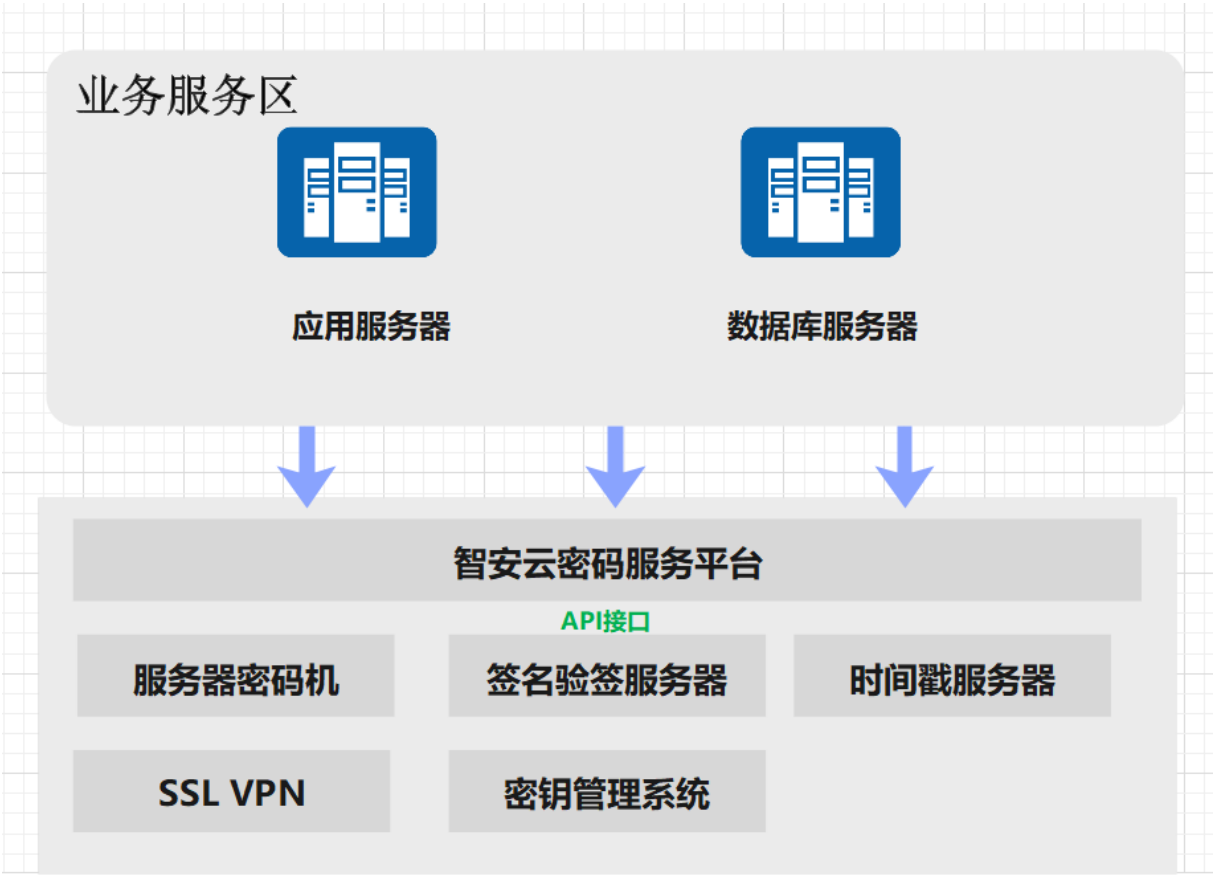

图 7-1 场景应用

智安云密码服务平台面向传统机房、IDC、公有云、私有云等环境，满足信息系统对密码资源的集中应用管理需求，能够向各类应用提供密码应用服务。典型应用场景包含公有云、私有云业务商密合规建设、政务云的密码资源池搭建及管理等。

8 关于我们

深圳市智安网络有限公司（简称：智安网络）是深圳市高新技术企业，下 设成都智安云御网络有限公司（安全运营中心）和深圳市智安网络有限公司南 京分公司（研发中心）两个子公司，成立于 2017 年 12 月 27 日，注册资本 2,000 万(元)。 作为安全运营中心，成都智安云御

网络有限公司（简称：智安云御）成立 于 2021 年 3 月，智安云御立足四川，放眼全球，坚持用户需求为导向，安全合 规为目标，自主研发为宗旨，力争成为云安全领域领先者，在数字时代为用户 的云安全及数据安全保驾护航。 智安云御基于企业安全能力模型 IPDRC（风险识别、安全防御、安全检测与 响应、安全管控）构建安全 API 即服务的能力，搭建了智安安全中台。