云密评专区

用户指南

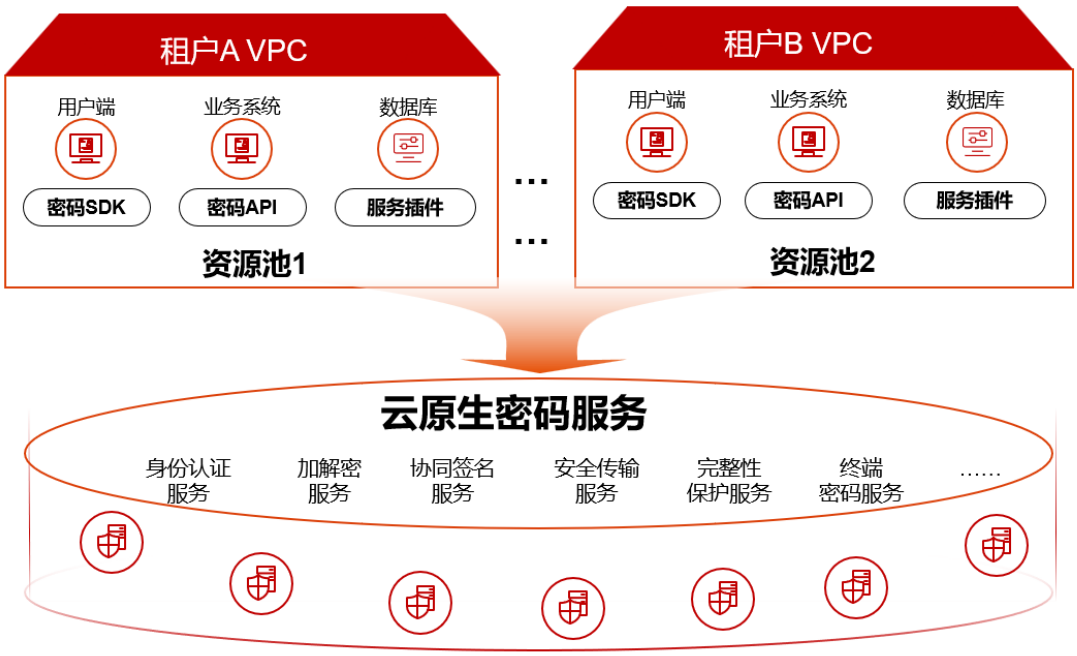
天翼云科技有限公司

目录

1 产品概述

1.1 产品介绍

云密评专区是针对云上租户密评需求提供的端到端密评产品解决方案，产品基于具有商密资质的云密码机、密码服务在云上构建高性能密码资源池，为应用提供密钥管理、综合安全网关、协同签名等云原生密码服务，解决云上应用密评方案复杂、改造时间长问题，帮助租户快速通过密评。



1.2 产品优势

满足密评合规

使用的产品都具备商用密码产品认证证书，为应用系统提供严格合规的密码服务，帮助应用系统通过密评

全场景密码服务

云密评专区提供全场景密码服务能力，包括重要数据加解密、身份认证、签名验签、协同签名等服务

应用快捷改造

提供统一标准的密码服务接口，应用改造简单快捷，具备完备的应用接入指南并提供及时、优质的技术支持服务

一站式专业服务

一对一专属项目经理，7*24H 技术支持，31 省本地化的销售网络体系，提供“家门口”的精细化客户服务。

1.3 功能特性

数据加解密

提供重要数据的加密和解密服务，满足密评中对重要数据传输和存储的机密性要求。

签名验签

提供重要数据的签名和验签服务，满足密评中对重要数据传输和存储的完整性要求以及操作的不可否认性要求。

密钥管理

提供集中的密钥全生命周期管理服务，满足密评中对密钥管理的安全性要求。

安全传输

提供网络通信通道的加密服务，满足密评中对网络和通信安全层面的数据传输机密性和完整性要求。

协同签名

配合移动端密码模块为应用系统移动端提供协同密码服务，满足应用终端身份认证、数据加密合规性要求

密评服务

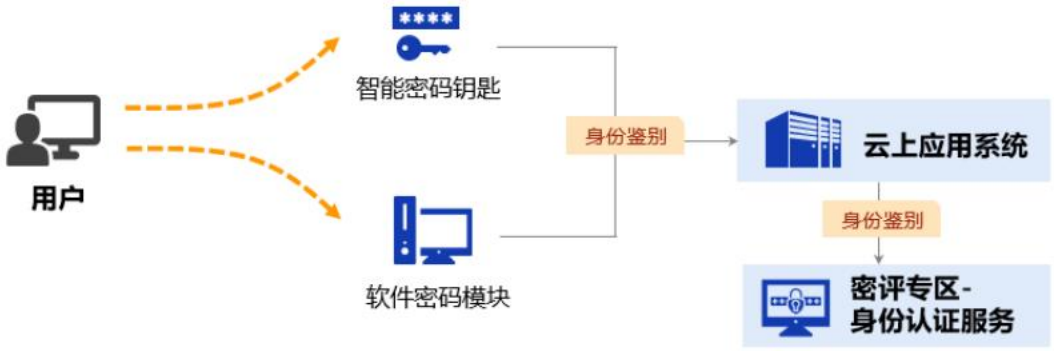
为租户侧提供密码方案设计、应用系统密改指导、应用系统密评支撑等服务

1.5 应用场景

云密评专区具有广泛的应用场景，本文为您介绍云密评专区常见的应用场景。

登录用户身份鉴别

密评中应用与数据安全层面的登录用户身份鉴别要求，应用系统的登录用户使用基于国密数字证书的身份认证服务，满足用户身份真实性要求。

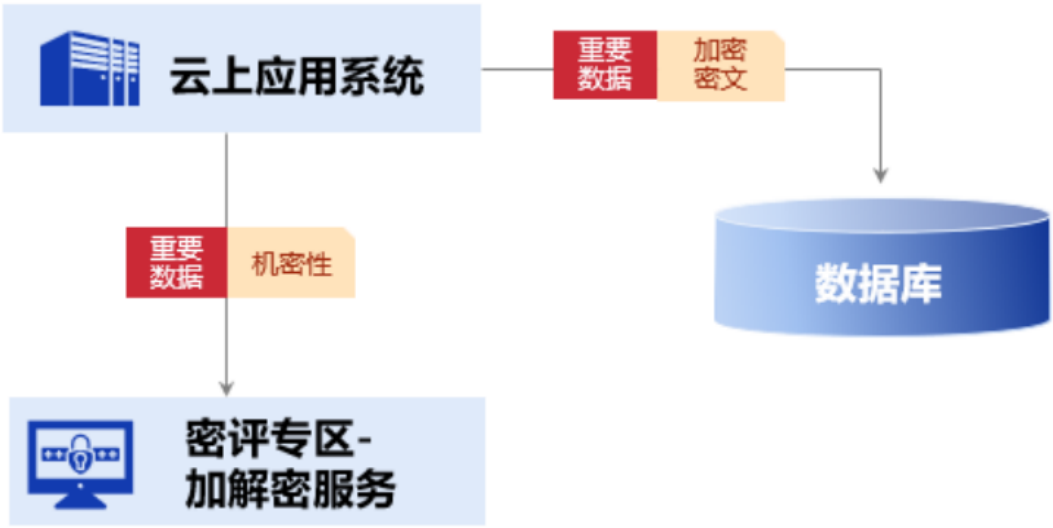


重要数据安全传输

密评中应用与数据安全层面的重要数据传输机密性和完整性要求，应用系统的重要数据在传输前调用云密评专区的数据加解服务、签名服务对数据进行机密性和完整性保护，传输完成后进行解密和验签，保障数据传输过程中的安全性。

重要数据加密存储

密评中应用与数据安全层面的重要数据存储机密性要求，应用系统的重要数据存储到数据库时需要进行加密保存，应用系统调用云密评专区的数据加密服务进行数据加密，把加密后的密文保存到数据库，满足数据存储机密性要求。



1.6 产品规格

云密评专区主要包含三大类计费内容，分为别密码产品、国密套件和密评服务。

密码产品

密码产品目前仅包含综合安全网关一个产品。

产品名称	计费模式
综合安全网关	包周期

国密套件

国密套件支持选购国密浏览器和密码钥匙两类产品。

说明：密码钥匙因需线下邮寄，所以该产品 10 个起售。

产品名称	计费模式
国密浏览器	按个计费
密码钥匙	按个计费

密评服务

此项为天翼云为您提供的密评相关的咨询服务，均为按次计费。

产品名称	计费模式
密评咨询服务	按次计费
密评测评服务（标准版）	按次计费
密评测评服务（企业版）	按次计费
密码实施服务	按次计费

1.7 使用限制

网络访问限制

为避免网络故障或网络配置问题影响登录系统，请管理员优先检查网络配置是否允许访问产品实例，并参考下表配置实例安全组。

产品名称	端口	端口用途
综合安全网关	18443	使用综合安全网关的 SSL VPN 服务必开的端口。
综合安全网关	18444-18454	此端口范围为您新增网关安全服务时预留的端口范围，请您按需选择。

综合安全网关网络限制条件

您需要在对接综合安全网关实例的安全组下放通以下 IP，否则无法正常使用：

- 100.89.0.0/16

如何添加安全组规则请参考：添加安全组规则章节。

数据加密网关支持的数据库及版本

数据库类型	**支持数据库版本**
MySQL	5.7、8.2.0
Mariadb	10.3.35、10.4、11.2.2
Oracle	11g、19c、23c、rac
SqlServer	2008、2016、2022

数据库类型	支持数据库版本
Percona	8
Oracle	11g、19c、23c、19c-RAC
Postgres	8.4、16.1
Greenplum	7
Opengauss	5.0.0
TiDB	6.5.5
Oceanbase	3.1.0
瀚高 Higo	6.0.4
人大金仓 Kingbase	V8、V9
海量数据库 Vastbase	g100
亚信安慧 Antdb	7.2.0
南大通用 Gbase	8c
云和恩墨 MogDB	5.0.0

数据库类型	支持数据库版本
神舟通用	opengauss 版
达梦	7、8

2 计费说明

2.1 计费项

云密评专区主要包含三大类计费内容，分为别密码产品、国密套件和密评服务。

说明：

云密评专区目前仅支持以下资源池购买及部署：

上海 33、西南 1、华北 2、华南 2、华东 1。

密码产品

密码产品目前包含综合安全网关、协同签名服务和数字证书认证系统三个产品，具体计费价格参考下表。

产品名称	计费模式	标准版价格	一年付价格	二年付价格	三年付价格
综合安全网关	包周期	6000 元/月	61200 元/年	122400 元/2 年	183600 元/3 年
协同签名服务	包周期	4000 元/月	40800 元/年	81600 元/2 年	122400 元/3 年
数字证书认证系统	包周期	5000 元/月	51000 元/年	102000 元/2 年	153000 元/3 年

国密套件

国密套件支持选购国密浏览器和密码钥匙两类产品，具体计费价格参考下表。

产品名称	计费模式	标准版价格
国密浏览器	一次性计费	280 元
密码钥匙	一次性计费	150 元

密评服务

产品名称	计费模式	版本价格
密评咨询服务	按个计费	60000 元/个

产品名称	计费模式	版本价格
密评测评服务（标准版）	按个计费	120000 元/个
密评测评服务（企业版）	按个计费	270000 元/个
密评改造服务	按个计费	55000 元/个

2.2 业务选购

若您需要购买云密评专区的相关业务，可参考本章节进行选购。

说明：

云密评专区目前仅支持以下资源池购买及部署：

上海 33、西南 1、华北 2、华南 2、华东 1。

选购步骤

1.登录云密评专区管理控制台。

2.单击右上角的“订购云密评专区”，跳转至选购页面。

3.选择需要购买的业务及各项配置。

配置项		**配置项说明**
地域		**选择您业务所需要部署的资源池。**
密码产品	**综合安全**	**选择需要购买综合安全网关的个数，最大仅支持购买**

配置项		配置项说明
	网关服务	10 个。 服务说明请参考：功能特性章节。 计费价格请参考：计费项章节。
国密套件	国密浏览器	选择需购买的国密浏览器个数，兼容主流国产操作系统，满足国密安全传输要求。
	密码钥匙	选择需购买的密钥钥匙个数，10 个起售。
密评服务	密评咨询服务	为应用设计密码应用方案，协助密评机构开展密评，单个应用配置 1 套。
	密评测评服务	支持 1 个应用密码应用安全性评估。
	密码改造服务	项目特殊需求定制服务，下单前请提前和产品经理沟通并评估工作量，根据工作量确定下单数量。
企业项目		选择此次购买的密评服务所属的企业项目，方便您进行管理。
虚拟私有云		选择密码产品实例所要配置的虚拟私有云。 注意

配置项		配置项说明
		成功创建后，VPC 不可更换，请谨慎选择
安全组		选择密码产品实例所在的安全组。
子网		选择密码产品实例所属的子网。 说明 暂不支持 IPv6 子网
密码产品管理员账号初始账密	用户名	设置购买的密码产品实例管理员初始账号。
	密码	设置购买的密码产品实例管理员初始密码。
	确认密码	二次确认购买的密码产品实例管理员初始密码。
购买时长		选择购买密码产品的时长。

4.配置完成后，勾选“我已阅读并同意《天翼云云密评专区服务协议》《隐私政策声明》”后，单击“提交订单”。

2.3 续订及退订

- **续订**：请联系您的专属客户经理进行续订，如果没有专属客户经理，可拨打天翼云客服电话 4008-109-889 咨询。
- **退订**：请联系您的专属客户经理退订，如果没有专属客户经理，可拨打天翼云客服电话 4008-109-889 咨询。

3 快速入门

3.1 云密评专区—综合安全网关快速入门

新增网关服务证书

说明：

一个综合安全网关实例仅支持创建一个网关服务证书，若您的服务已创建证书则无法再新增。

1.登录综合安全网关实例。

2.在左侧导航栏选择“SSL 网关服务 > 网关服务证书”，单击页面左上角的“新增证书”按钮。

3.在弹出的“新增网关服务证书”对话框中，选择需要新增的证书规格。

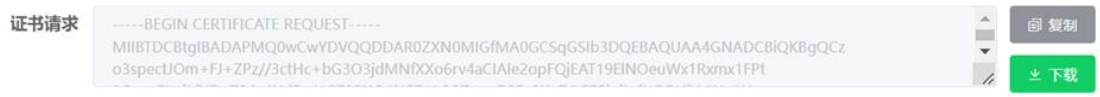
4.选择完成后，单击“确定”完成证书新增。

生成证书 CSR

1.选择需要生成 CSR 的证书，单击“操作”列的“CSR 请求”按钮。

2.在弹出的对话框中配置 CSR 相关内容。

3.配置完成后，单击“生成证书请求”，会在“证书请求”栏中生成 CSR。



4.根据您业务自身需求选择复制保存或者下载文件保存。

新增网关服务并配置

1.登录综合安全网关实例。

2.在左侧导航栏选择“SSL 网关服务 > 网关服务管理”，在页面左上角单击“开通网关服务”。

3.在弹出的“新增网关服务”的对话框中配置网关服务参数。

4.确认填写的内容后，单击“确定”完成新增网关服务。

5.配置完成后返回到“网关服务管理”页面，单击“操作”列的“配置”按钮开始配置网关。

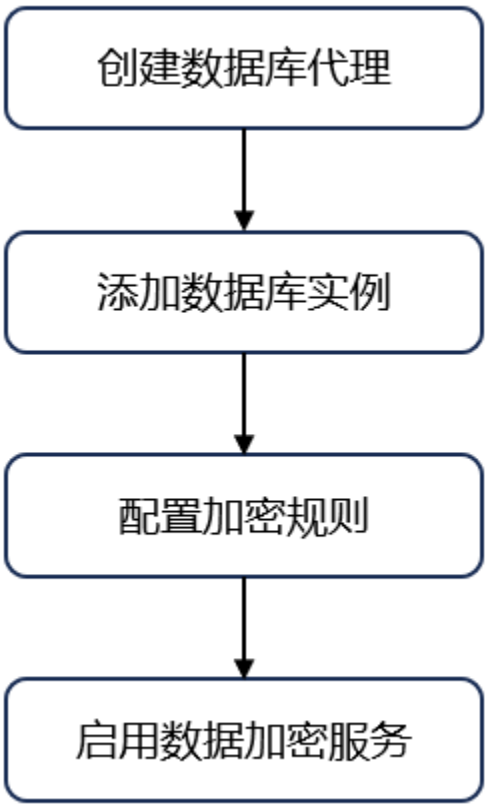
6.在弹出的“配置网关服务”对话框中，配置相关参数。

3.2 云密评专区—数据加密网关快速入门

基于透明化服务理念，业务应用无需改造即可实现数据库中敏感数据的保护，支持国密算法，保证存储过程的机密性和完整性，满足应用和数据安全的合规要求。

启用流程

数据加密网关启用流程大致可参考下图：



步骤一：创建数据库代理

1.使用运维账号登录数据加密网关。

2.在左侧导航栏选择“数据库管理 > 数据库列表”，进入“数据库列表”页面。

3.单击页面左上角的“新增”按钮，进入“新增代理实例”页面。

4.填写数据库实例代理相关内容，填写完成后单击“提交”，即可完成数据库代理配置。

步骤二：添加数据库实例

1.使用运维账号登录数据加密网关。

2.在左侧导航栏选择“数据库管理 > 数据库列表”，进入“数据库列表”页面。

3.单击“操作”列的“新增实例”按钮，跳转至“新增实例”页面。

4.填写相关参数，将实例纳管至数据库代理中。

步骤三：配置加密规则

1.选择需要配置加密规则的数据库，单击“操作”列的“配置加密”。

2.在“表名”下拉框中选择需要配置加密规则的数据库表。

3.单击“加密配置”，选择需要加密的字段开始配置。

步骤四：启用数据加密服务

配置完成后，单击对应数据库实例的“加密洗数”即可开始使用数据加密服务。

4 用户指南

4.1 密码产品实例

操作步骤

1.登录天翼云官网，单击证书管理服务产品详情页。

2.单击【立即订购】，进入到证书管理服务产品购买页面。

3.输入域名购买方式：填写域名名称，选择证书规格以及购买时长，若您不知道域名可以单击“快速购买方式”切换。

4.SSL 证书数量购买方式：选择证书数量、规格以及购买时长，具体的规格选择可参见下表。

证书规格	适用场景	说明
域名型证书（DV）	如果您的网站主体是个人（即没有企业营业执照），只能申请域名型（DV）证书。	信任等级一般，只需验证域名的真实性便可颁发证书保护网站，签发证书速度最快，一般申请通过验证后几分钟即可获取到证书。
企业型证书（OV）	对于一般企业，建议购买 OV 型及以上类型的 SSL 证书。（若作为移动端网站或接口调用，也建议您购买 OV 型及以上类型的 SSL 证书。）	信任等级较高，必须要验证域名权限以及企业的身份，审核严格，安全性高。
增强型证书（EV）	对于金融、支付类企业，建议购买 EV 型证书。	信任等级强，一般用于银行证券等金融机构、大中型企业等，审核更严格，安全性更高，同时在浏览器显示公司名称。

说明：

若您选择购买服务的时长为 2 年期，那么此服务中包含 2 张有效期为 1 年的 SSL 证书，在到期 30 天前，天翼云将会自动为您续期证书。

5.阅读天翼云《证书管理服务协议》后，勾选我已阅理解并接受，即可单击“立即购买”下单。

6.单击“提交订单”，在弹出的“订单详情”页确认订单信息。

7.单击“立即支付”，完成 SSL 证书的购买。

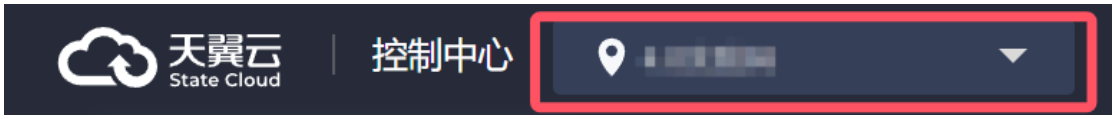
4.1.1 登录实例

在您购买云密评专区的密码服务后，会在控制台生成所选购服务的实例，下面为您介绍如何登录实例。

登录步骤

1.登录天翼云云密评专区控制台。

2.在界面左上角选择部署业务的资源池，进入实例界面。



3.选择要登录的实例，单击“管理 > 从外（内）网地址登录”。

说明：

- 从外网地址登录需要您为该实例绑定弹性 IP，并且弹性 IP 可使用。
- 从内网地址登录需要您和内网网络互通才可访问。

4.2 云密评专区-综合安全网关实例

开通堡垒机（原生版）后，用户在控制台 “云堡垒机实例”页面，在操作列点击“管理”操作，系统单点登录进入云堡垒机实例，通过控制台登录进入默认管理员用户。

登录的时候可选“外网地址登录”或“内网地址登录”。

说明

- 内网地址登录需要确保网络环境互通。
- 外网地址登录需要绑定弹性 IP。

首次登录

在未设置初始密码时，需通过云堡垒机控制台单点登入跳转登入堡垒机，并进行初始化管理操作。

1.在“云堡垒机实例”列表条目录中选择要管理的实例，单击“管理”。

2.根据您自身的网络环境选择“内网地址登录”或“外网地址登录”。

3.登入堡垒机后，通过个人信息进行初始密码设置。

4.2.1 登录综合安全网关实例

综合安全网关是一款专为解决网络间安全互联而设计的高性能安全产品。

它基于 SSL 协议，能够在不可信的公共网络上建立安全、加密的通信隧道，确保数据的机密性和完整性。

该产品提供了强大的身份认证机制，支持多种认证方式，如密码、智能卡和生物识别等，有效防止未经授权的访问。

此外，综合安全网关还具有灵活的访问控制策略，可以根据用户身份和设备类型授予不同的访问权限，保护企业内部资源的安全。它易于部署和管理，支持各种操作系统和移动设备，满足远程办公和移动办公的需求，广泛应用于企业、政府机构和教育领域。

您成功购买综合安全网关实例后，可在天翼云云密评专区管理控制台或者通过绑定的 EIP 地址登录。

开放端口要求

为避免网络故障或网络配置问题影响登录系统，请管理员优先检查网络配置是否允许访问综合安全网关，并参考下表配置实例安全组。

注意：

您需要在对接综合安全网关实例的安全组下放通以下 IP：

100.89.0.0/16

如何添加安全组规则请参考：添加安全组规则章节。

端口	端口用途
18443	使用综合安全网关的 SSL VPN 服务必开的端口。
18444- 18454	此端口范围为您新增网关安全服务时预留的端口范围，请您按需选择。

通过天翼云控制台登录

1.登录天翼云云密评专区管理控制台。

2.在左侧导航栏选择“密码服务”，进入“密码服务”页面。

3.选择需要登录的综合网关实例，选择“管理 > 从外（内）网地址登录”。

说明

- 选择“从外网地址登录”需要实例绑定可用的弹性 IP。
- 选择“从内网地址登录”需要确保您的网络环境可以访问内网。

4.2.2 SSL 网关服务

成功购买证书后，您需要申请证书，即为证书绑定域名或 IP、填写证书申请人的详细信息并提交审核。所有信息通过审核后，证书颁发机构才签发证书。

前提条件

已成功购买证书并且在控制台的“证书状态”为“待申请”。

操作步骤

1.登录“证书管理服务”控制台，在左侧导航栏选择“我的证书 > 证书管理”，随后在顶部导航栏选择“可申请”，进入“证书管理”页面。

2.选择“企业型（OV）SSL”或“增强型（EV）SSL”证书，单击“操作”列的“证书申请”按钮，进行 SSL 证书申请。

3.在右侧的对话框中填写证书申请的相关信息。

填写参数	参数说明
证书绑定域名	第一个域名将作为证书通用域名名称（不可修改）
域名验证方式	可选“手工 DNS 验证”或“文件验证”。 “文件验证”目前仅支持绑定 IP 方式的 OV 证书验证。
联系人	选择联系人，如何新建联系人请参考信息管理章节。
公司	选择公司，如何新建公司请参考信息管理章节。

填写参数	参数说明
所在地	根据所选择的公司所在地自动生成。
密钥算法	可选择“RSA”、“ECC”或“SM2”（根据购买证书页面所选的加密标准选择）
CSR 生成方式	可选择“系统生成”或“手动生成”。

注意：

- 为保障您的证书顺利申请，建议您使用系统生成 CSR 的方式，手动上传将无法署到天翼云产品。建议您使用系统创建的 CSR，避免因内容不正确而导致的审核失败。
- 若您选择手动生成 CSR，使用已创建的 CSR 申请证书，请不要在证书签发完成前删除 CSR。

4. 填写完后，单击“提交审核”。

5.进行人工验证环节，单击“下载确认函模板”。(仅支持企业型(OV)/增强型(EV)SSL 证书)

6.查看下载的确认函，若确认无误选择该确认函文件上传，单击“点击上传”进行上传。

说明：

- 确认函需要在模板标黄处填写内容，并在公司名称处盖章后回传。
- 若您申请的是国密证书，还需在填写公司对公账户的开户行名称、对公账户账号及公司地址。
- 如果您申请证书时填写邮箱企业邮箱与企业域名相关（例如申请的域名为*.ctyun.com，企业邮箱为*@chinatelecom.com），并且该企业邮箱可以正

常收发外部邮件，这种情形下可以不提供确认函。

- 企业发送工商登记年报的邮箱若可以正常收发外部邮件，使用该邮箱申请证书时可以不提供确认函。
- 非以上场景申请企业型（OV）和增强型（EV）证书必须提供确认函，建议使用 189、126、163、QQ 等免费邮箱。

7 配置域名验证信息，配置域名信息操作可参考域名验证，配置完成后等待审核签发证书。

8.若证书已成功签发，可返回到“已签发”页签查看签发成功的证书。

4.2.2.1 功能概述

网关服务管理：用于维护网关服务，提供开通网关服务，删除，配置，查询详情等功能。

网关服务器组：SSL 网关服务功能的具体实现是由网关服务器实现的，而网关服务器则由网关服务器组统一管理，网关服务与网关服务器组是 1 对 1 的关系，提供服务器组的新增，编辑，删除，查看服务器列表，以及服务器的添加，修改，删除，启用/停用等功能。

网关服务证书：SSL 网关服务使用网关服务证书来进行安全认证工作，使用 SSL 网关服务的前提是必须安装相关网关服务证书，提供新增，查看详情，启用，停用，可信证书链管理，CSR 请求，证书应答，导入证书等功能。

网关服务优化策略：用于优化外部应用访问。

4.2.2.2 网关服务器管理

网关服务器组是 SSL 网关服务功能的具体实现是由网关服务器实现的，而网关服务器则由

网关服务器组统一管理，网关服务与网关服务器组是一对一的关系，提供服务器组的新增，编辑，删除，查看服务器列表，以及服务器的添加，修改，删除，启用/停用等功能。

新增服务器组

1.登录综合安全网关实例。

2.在左侧导航栏选择“SSL 网关服务 > 网关服务器组”，单击页面左上角的“新增服务器组”。

3.在弹出的对话框中填写相关内容。

参数	参数说明
分组名称	自定义服务器组的名称。
服务类型	选择服务器组的服务类型。

4.确认后单击“确定”即完成创建。

后续操作

编辑服务器组：选择需要编辑的服务器组，单击“操作”列的“编辑”即可修改。

删除服务器组：选择需要删除的服务器组，单击“操作”列的“删除”即可删除服务器组。

4.2.2.3 网关服务器组管理

添加服务器

1.登录综合安全网关实例。

2.在左侧导航栏选择“SSL 网关服务 > 网关服务器组”，选择需要添加服务器的服务器组，

单击“操作”列的“添加密码机”。

3.在弹出的对话框中配置服务器的参数。

参数	参数说明
IP	填写密码机的 IP 地址。
端口	填写密码机的端口。
权重	选择密码机的权重。
描述	自定义密码机的描述。
启用	选择添加后密码机的启用状态。

4.填写完成后，单击“确定”完成服务器添加。

后续操作

启停服务器：点开服务器所在的服务器组，选择需要编辑的服务器，单击“操作”列的“启用/停用”即可启停服务器。

编辑服务器：点开服务器所在的服务器组，选择需要编辑的服务器，单击“操作”列的“编辑”即可修改。

删除服务器：点开服务器所在的服务器组，选择需要删除的服务器组，单击“操作”列的“删除”即可删除服务器。

4.2.2.4 网关服务证书管理

网关服务证书是 SSL 网关服务使用网关服务证书来进行安全认证工作，使用 SSL 网关服务的前提是必须安装相关网关服务证书，提供新增，查看详情，启用，停用，可信证书链管理，CSR 请求，证书应答，导入证书等功能。

新增证书

说明：

一个综合安全网关实例仅支持创建一个网关服务证书，若您的服务已创建证书则无法再新增。

1.登录综合安全网关实例。

2.在左侧导航栏选择“SSL 网关服务 > 网关服务证书”，单击页面左上角的“生成证书请求”按钮。

3.在弹出的“新增网关服务证书”对话框中，选择需要新增的证书规格。

参数	参数说明
密钥识别名	根据您证书填写的证书识别名自动填写，无法修改。
密钥算法	根据您证书填写的证书算法自动填写，无法修改。
证书请求类型	自动填写证书请求类型，无法修改。
密钥长度	根据您的需求选择密钥的长度。
请求签名算法	在下拉框中选择请求签名算法。

参数	参数说明
公钥指数	根据业务需求选择公钥指数。
主题格式	选择主题格式，支持“标准主题”和“自定义主题”。
通用名	仅选择“标准主题”时需填写，填写 CSR 的通用名。
自定义主题	仅选择“自定义主题”是需填写，根据业务自身需求填写主题内容。

4.选择完成后，单击“确定”完成证书新增。

后续操作

启用/停用证书：选择需要启用/停用的证书，单击“操作”列的“启用/停用”按钮，即可完成启用/停用。

添加可信证书链

1.选择需要添加可信证书链的证书，单击“操作”列的“可信证书链”，进入“可信证书链”页面。

2.单击页面左上角的“添加可信证书”按钮，弹出“添加可信证书”对话框。

3.上传正确的证书文件后，单击“确定”完成添加。

说明

只支持上传.cer/.p7b/.der 格式的文件，每次操作仅支持上传单个文件。

4.2.2.5 网关服务优化策略

网关服务优化策略可以用于优化外部应用访问。

新增优化策略

1.登录综合安全网关实例。

2.在实例页面左上角单击“新增优化策略”。

3.在弹出的对话框中配置相关参数。

参数	参数说明
策略名	自定义需要新增的优化策略名。
IO 超时	设置网关策略的 IO 超时值。
压缩	选择是否开启压缩。
缓存	选择是否开启缓存。
连接复用	选择是否开启连接复用。

4.配置完成后单击“确定”即可完成新增。

后续操作

编辑优化策略：选择需要编辑的网关服务优化策略，单击“操作”列的“编辑”，在弹出的对话框中修改相关配置，编辑完成后单击“确定”即完成修改。

4.2.3 SSLVPN 服务

4.2.3.6 功能概述

VPN 服务管理：用于维护 VPN 服务，提供配置 VPN 服务；对内网控制新增和删除；对静态路由表的新增，修改，删除等功能。

VPN 服务证书：SSL VPN 服务使用 VPN 服务证书来进行安全认证工作，使用 SSL VPN 服务的前提是必须安装相关 VPN 服务证书，提供新增，查看详情，启用，停用，可信证书链管理，CSR 请求，证书应答，导入证书等功能。

4.2.3.7 VPN 服务证书

VPN 服务证书是进行安全认证工作的必要条件，使用 SSL VPN 服务的前提是必须安装相关 VPN 服务证书，综合安全网关提供新增、查看详情、启用、停用、可信证书链管理、CSR 请求、证书应答、导入证书等功能。

生成证书请求

1.登录综合安全网关实例。

2.在左侧导航栏选择“VPN 服务 > VPN 服务证书”，进入“VPN 服务证书”页面。

3.单击页面右上角的“生成证书请求”按钮。

4.在弹出的“生成证书请求”对话框中，配置相关内容。

参数	参数说明
密钥识别名	自定义密钥匙别名。

参数	参数说明
密钥算法	目前仅支持“SM2”密钥算法。
证书请求类型	选择证书请求类型。
主题格式	选择主题格式，支持“标准主题”和“自定义主题”。
标准主题	仅选择“标准主题”时需填写，仅 CSR 通用名为必填项。
自定义主题	仅选择“自定义主题”是需填写，根据业务自身需求填写主题内容。

5.配置完成后，单击“生成证书请求”，会在控制台中生成最新的服务证书及证书请求文件。

后续操作

启用/停用证书：选择需要启用/停用的证书，单击“操作”列的“启用/停用”按钮，在弹出的对话框中单击“确定”，即可完成“启用/停用”操作。

可信证书链

VPN 服务证书的可信证书链，需要在选择 VPN 服务证书信息后才可添加相关内容

添加可信证书链

1.选择需要添加可信证书链的证书，单击“操作”列的“可信证书链”，进入“可信证书链”页面。

2.单击页面左上角的“添加可信证书”按钮，弹出“添加可信证书”对话框。

3.上传正确的证书文件后，单击“确定”完成添加。

说明：

只支持上传.cer/.p7b/.der 格式的文件，每次操作仅支持上传单个文件。

删除可信证书链

1.选择需要删除可信证书链的证书，单击“操作”列的“可信证书链”，进入“可信证书链”页面。

2.选择需要删除的证书链，单击“操作”列的“删除”按钮。

3.在弹出的对话框中单击“确定”即可完成删除。

下载可信证书链

1.选择需要下载可信证书链的证书，单击“操作”列的“可信证书链”，进入“可信证书链”页面。

2.选择需要下载的证书链，单击“操作”列的“下载证书”按钮即可下载。

4.2.3.8 VPN 服务管理

VPN 服务管理提供以下功能：

- 提供配置 VPN 服务；
- 对内网控制新增和删除；
- 对静态路由表的新增，修改，删除等。

前提条件

为保障您的 SSL VPN 服务正常使用，需要在综合安全网关实例所属的安全组中放通 18443 端口。

新增 VPN 服务管理

说明：

您在首次登录 VPN 服务页面，界面会提示“该 SSL VPN 服务尚未配置”。

1.登录综合安全网关实例。

2.在左侧导航栏选择“VPN 服务 > VPN 服务管理”，进入“VPN 服务管理”页面。

3.开始配置“VPN 服务”，完成配置后单击“配置”按钮即可完成修改。

参数	参数说明
Vpn 服务 uid	系统自动生成，无需填写。
服务名称	自定义 VPN 服务的名称。
证书	选择 VPN 服务的证书，证书的添加请参加：VPN 服务证书章节。
SSL 协议	选择 VPN 服务对应的 SSL 协议，第一次配置后无法修改。
SSL 算法	选择 VPN 服务对应的 SSL 算法，第一次配置后无法修改。
服务端口	填写 VPN 服务对应的端口，第一次配置后无法修改。

新增内网控制

1.登录综合安全网关实例。

2.在左侧导航栏选择“VPN 服务 > VPN 服务管理”，进入“VPN 服务管理”页面。

3.选择“内网控制”页签，单击“创建内网”按钮。

4.在弹出的对话框中填写“IP 地址”或“IP 网段”。

5.填写完成后单击“确定”即可新增内网控制。

新增静态路由

1.登录综合安全网关实例。

2.在左侧导航栏选择“VPN 服务 > VPN 服务管理”，进入“VPN 服务管理”页面。

3.选择“静态路由表”页签，单击“创建路由”按钮。

4.在弹出的对话框中配置静态路由的相关内容。

参数	参数说明
IP 地址	填写静态路由的 IP 地址。
网关	填写静态路由的网关。
子网掩码	填写静态路由的子网掩码。
网口	填写静态路由的网口。
添加位置	选择静态路由配置所处的位置。

5.单击“确定”完成新增静态路由。

后续操作

修改静态路由信息：选择需要修改的静态路由信息，单击“操作”列的“修改”即可修改静态路由的相关信息。

删除静态路由信息：选择需要删除的静态路由信息，单击“操作”列的“删除”即可删除静态路由。

4.2.4 日志审计

日志审计功能是记录机构用户的操作日志，并提供查看详情，审核，批量审核，验签等功能。

查看日志操作记录并审核

1.登录综合安全网关实例。

2.在左侧导航栏选择“管理审计日志”，进入“管理审计日志页面”。

3.查看“操作名称”列的操作情况，进行审计。

4.单击“操作”列的“验签”按钮，若验签成功则单击“审核”按钮进行审计。

导出日志

1.登录综合安全网关实例。

2.在左侧导航栏选择“管理审计日志”，进入“管理审计日志页面”。

3.若您需要导出所有日志可单击“导出全部”按钮，若您需要导出部分日志可勾选需要导出的日志后单击“导出所有按钮”。

4.2.5 系统管理

4.2.5.9 用户管理

用户管理是指管理当前实例下所有用户信息，提供新增、编辑、Ukey 绑定、重置等功能

新增用户

1.登录综合安全网关实例。

2.选择“系统管理 > 用户管理”，进入“用户管理”页面。

3.单击页面左上角的“添加用户”，在弹出的“添加用户”窗口中配置用户参数。

参数	参数说明
登录名	自定义用户的登录名，配置后不可修改。
别名	（选填）设置用户的别名。
角色	选择该登录用户在系统中的角色。
手机号码	（选填）填写手机号。
邮箱地址	（选填）填写新增用户的邮箱地址。
地址	（选填）填写新增用户的地址。

4.配置完成后，单击“确定”完成用户添加。

后续操作

编辑用户：选择需要编辑的用户，单击“操作”列的“编辑”按钮，修改用户的相关信息后

单击“确定”完成修改。

绑定 UKey：选择需要绑定 UKey 的用户，单击“操作”列的“UKEY 绑定”按钮，在弹出的对话框中填写 UKEY 序列号及 PIN 码完成绑定。

解绑 UKey：选择需要解除绑定 UKey 的用户，单击“操作”列的“UKEY 解绑”按钮，在弹出的对话框中填写及 PIN 码完成解绑。

重置用户密码：选择需要重置密码的用户，单击“操作”列的“重置口令”按钮，在弹出的对话框中单击“确定”完成重置。

4.2.5.10 UKEY 管理

UKEY 模块提供 UKEY 管理的相关功能，如：UKEY 初始化、UKEY 信息查询和备份历史查询等。

说明：

首次使用 UKEY 需要在综合安全网关登录页面下载 UKEY 插件。

UKEY 初始化

1.登录综合安全网关实例。

2.在左侧导航栏选择“系统管理 > UKEY 管理”，进入 UKEY 管理页面。

3.单击“UKEY 初始化”，进入 UKEY 初始化步骤。

4.将 UKEY 设备连接，单击“刷新”按钮获取 UKEY 序列号。

5.获取 UKEY 序列号后，输入 PIN 码并且二次输入进行确认完成初始化。

6.重复第 4 步和第 5 步操作，完成后续步骤。

查看 UKEY 信息

1.登录综合安全网关实例。

2.在左侧导航栏选择“系统管理 > UKEY 管理”，进入 UKEY 管理页面。

3.选择“UKEY 信息”即可查看已经对接的信息。

4.3 云密评专区-数据加密网关实例

4.3.1 数据加密网关概述

数据加密网关是一种专门为保护数据库数据存储安全而设计的高性能密码设备。它基于数据加密技术，能够在数据进入数据库之前对其进行加密处理，从而确保数据的机密性和完整性。这款创新设备在当今数据安全需求日益增长的环境下，扮演着至关重要的角色。

核心功能与优势

数据加密 ：数据库加密网关采用先进的加密算法，对数据进行实时加密。无论是静态数据还是传输中的数据，都能得到有效保护，防止未经授权的访问和数据泄露。

高性能处理 ：作为一款高性能密码网关设备，它具备出色的处理能力，能够在保证数据安全的同时，不降低数据库的读写性能。这使得它在处理大量数据时依然能够保持高效稳定。

密钥管理 ：内置完善的密钥管理系统，能够安全地生成、存储和管理加密密钥。密钥的严密管理是数据安全的重要保障，防止密钥泄露导致的数据风险。

透明加密 ：提供透明的加密服务，应用程序无需改动即可享受数据加密保护。数据库加密网关在后台自动完成加密和解密操作，简化了数据安全管理。

兼容性强 ：支持多种数据库系统和应用程序，无需对现有系统进行大规模改造即可部署。这使得它能够快速融入企业现有的 IT 架构，提供即时的数据安全防护。

通过天翼云控制台登录

1.登录天翼云云密评专区管理控制台，选择产品部署的资源池。

2.在左侧导航栏选择“密码服务”，进入“密码服务”页面。

3.选择需要登录的数据加密网关实例，选择“管理 > 从外（内）网地址登录”。

说明：

选择“从外网地址登录”需要实例绑定可用的弹性 IP。

选择“从内网地址登录”需要确保您的网络环境可以访问内网。

4.3.2 数据库管理

证书管理服务支持将已签发的证书一键部署至您的服务器上，减少您去手动部署证书的相关操作，提升业务的便捷性。

约束限制

- 只有已签发的证书支持一键部署功能
- 当前仅支持将证书部署到 Web 应用防火墙（原生版）
- 不支持国密规格证书的一键部署
- 仅支持通过**证书管理服务**控制台签发的证书使用一键部署功能。

操作步骤

1.登录“证书管理服务”控制台，在左侧导航栏选择“我的证书 > 证书管理”，进入“证书管理”页面。

2.在导航栏选择“已签发”，筛选出已经成功签发的证书。

3.选择需要部署的证书，选择“操作”列的“更多 > 一键部署”。

4.在右侧弹出的对话框中，在下方选择需要部署的证书，单击“操作”列的“部署”或“重新部署”，即可完成证书的部署。

说明：

您可以批量勾选需要部署的证书（最多支持 5 个整数），单击“批量部署”。

后续操作

查看部署记录：选择“部署记录”，可查看该证书的历史部署情况和回退情况。

回退：在部署记录中找寻需要回退的证书及部署时间，单击“操作”列的“回退”即可回退。

4.3.2.11 数据库列表

代理管理

数据库加密机网关对数据库的加解密是通过解析改写数据库二进制协议实现的。

本章节将指导您如何将您的数据库服务纳入数据加密网关管理之下。

新增数据库代理

1.使用运维账号登录数据加密网关。

2.在左侧导航栏选择“数据库管理 > 数据库列表”，进入“数据库列表”页面。

3.单击页面左上角的“新增”按钮，进入“新增代理实例”页面。

4.填写数据库实例代理相关内容，填写完成后单击“提交”，即可完成数据库代理配置。

参数	参数说明
数据库类型	根据您自身的业务需求选择数据库类型，具体支持选择的数据库类型请参考使用限制章节。
数据库版本	选择数据库版本号，具体支持的数据库版本请参考使用限制章节。
实例 IP	填写物理数据库的 IP 地址，请确保填写的 IP 地址准确。
实例端口	填写物理数据库连接端口，请确保填写的实例端口准确。
代理端口	自定义代理数据库的服务端口。
是否大小写敏感	选择是否敏感，请根据物理数据库实际情况选择。
实例类型	选择“单节点”或者“主从”，请确认您的数据库部署方式正确选择。 当您选择“主从”时，需要填写关联实例的 IP、端口和代理端口信息。 - 单节点：单节点是指是指数据库软件安装在一台服务器上。 - 主从：主从是指数据库软件安装在两台或多台服务器上
描述	对新建的代理服务进行描述。
模式名包裹符号	与物理数据库保持一致。

参数	参数说明
字段值包裹符号	与物理数据库保持一致。
密文数据格式	根据您自身的业务需求选择“base64”或“hex”。
通配符	自定义通配符。

后续操作

开启/关闭代理：单击“操作”列的“开启/关闭代理”，可以控制代理数据库的开启和关闭状态，开启代理之后，应用即可将 JDBC 连接从物理数据库上切换至代理数据库上。

开启/关闭仿真模式：选择“操作”列的“仿真 > 开启/关闭”，仿真模式下，代理数据库将会把应用产生的数据 SQL 根据配置的规则进行解析后，存入仿真文件中，由应用判断改写后的 SQL 是否符合要求。

实例管理

在添加数据库代理后，可以将您的数据库实例添加至数据库代理下管理。

添加数据库实例

1.使用运维账号登录数据加密网关。

2.在左侧导航栏选择“数据库管理 > 数据库列表”，进入“数据库列表”页面。

3.单击“操作”列的“新增实例”按钮，跳转至“新增实例”页面。

4.填写相关参数，将实例纳管至数据库代理中。

参数	参数说明
用户名	填写物理数据库登录用户名
用户口令	填写物理数据库登录用户的口令
实例库名称	填写物理数据库的实例名称
加密密钥	选择加密密钥，若首次添加数据库实例，建议选择“新建加密密钥”。
JDBC URL 参数	根据数据库特性配置参数。
描述	填写数据库实例的参数。

5.配置完成后单击“提交”即可完成数据库实例新增。

加密流程

步骤一：启用/禁用实例

禁用状态下，无法进行规则配置，且已经配置的规则将处于未生效的状态。

步骤二：配置加密规则

1.单击“实例 IP”前的箭头按钮，展开对应实例下的所有数据库实例。

2.选择需要配置加密规则的数据库，单击“操作”列的“配置加密”。

3.在“表名”下拉框中选择需要配置加密规则的数据库表。

4.单击“加密配置”，选择需要加密的字段开始配置。

加密规则：对指定表的指定字段进行加密规则配置，配置时可自定义密文字段的名称（密文字段用于存储密文数据），选择加密密钥、加密模式、补丁方式。

参数	**参数说明**
加密密钥	选择加密密钥，用于对明文数据进行加密
加密字段名称	选择加密字段名称，用于存储密文数据
加密模式	根据需求选择加密模式，支持选择一下三种： - ECB - CBC - FPE
补位方式	选择补位方式，目前仅支持：PKCS5Padding

完整性保护：对指定表的指定字段进行完整性保护规则配置，配置时可自定义完整性保护字段的名称（用于存储校验数据），选择加密密钥。

参数	**参数说明**
加密密钥	选择加密密钥，用于对明文数据生成校验值
加密字段名称	选择加密字段名称，用于存储校验值数据

模糊查询：对指定表的指定字段进行模糊查询规则配置，配置时可自定义模糊查询列的名称。

参数	参数说明
模糊查询字段名	自定义模糊查询列的名称

脱敏：对指定表的指定字段进行脱敏规则配置，配置了脱敏规则的字段可对数据进行脱敏处理。

参数	参数说明
脱敏算法	支持以下规则： - 保留前 N 后 M - 保留 X 到 Y - 遮盖前 N 后 M - 遮盖 X 到 Y - 特殊字符前遮盖 - 特殊字符后遮盖
替换字符	用于遮盖替换敏感数据

步骤三：载入配置

勾选完成“初始化密文列”操作的字段，单击“载入配置”。

此操作是确保您配置的规则进行加载生效。

步骤四：初始化密文列

完成加密规则配置后，单击“操作”列的“初始化密文列”。

可以选择复制 SQL 语句手动去物理库中执行，也可以选择一键执行。执行成功之后物理库会显示密文字段。

步骤五：加密洗数

注意：

进行加密洗数之前请确认仿真模式已关闭，仿真模式开启的情况下禁止加密洗数。

加密洗数是对物理数据库的存量明文数据按照相应的加密规则进行加密得到密文，将密文保存到相应的密文列中。

其他操作

完整性校验

完整性校验用来校验密文数据是否经过篡改。

完整性校验任务可以到任务列表中查看加密洗数任务完成状态以及洗数进度。

解密洗数

解密洗数是对物理数据库中的密文字段中的密文按照相应的加密规则进行解密得到原文数据保存在明文字段中。

解密完成后，此字段将不再被数据库加密网关进行管理，密文字段是否删除由用户评估后自行处理。

4.3.2.12 任务列表

任务列表用于展示洗数任务和完整性校验进度以及状态，并在洗数异常时提供下载异常信息

功能，帮助及时排查定位异常原因。

查询步骤

1.使用运维账号登录数据加密网关。

2.在左侧导航栏选择“数据库管理 > 任务列表”，进入“任务列表”页面。

3.选择需要查询的任务类型进行筛选。

4.3.3 密钥管理

密钥列表页面展示系统中当前所有的密钥及其属性，属性包括密钥来源、生成方式、密钥算法等。

新建密钥

1.使用运维账号登录数据加密网关。

2.在左侧导航栏选择“密钥管理“>“密钥列表” ，进入“密钥列表”页面。

3.单击“新增”，即可开始新增密钥，填写参数可参考下表

参数	参数说明
密钥名称	自定义密钥名称
密钥来源	选择密钥来源： - 密码设备 - KMS

参数	参数说明
密钥算法	选择密钥算法： - SM4 - AES - HMAC_SM3
生成方式	选择密钥生成方式
密钥因子	生成方式选择“派生”时生效

查询密钥

1.使用运维账号登录数据加密网关。

2.在左侧导航栏选择“密钥管理“>“密钥列表” ，进入“密钥列表”页面。

3.设置查询条件（密钥名称、密钥来源、生成方式），单击“查询”即可查询相关密钥。

4.3.4 日志管理

操作审计日志页面用来展示所有管理操作的日志，审计员可手动对每条日志执行审计。

数据库加密机支持操作日志完整性保护，在存储管理操作日志同时记录对应的完整性校验值，页面展示日志时会自动校验日志完整性，可有效防止非法用户恶意篡改操作审计日志。

查询审计日志

1.使用审计角色登录数据安全网关。

2.在菜单栏选择 “日志管理“>“审计日志列表” 进入审计列表页面。

3.设置查询条件（时间范围、操作用户、操作描述），单击“查询”即可查询相关审计日志。

审计日志

1.使用审计角色登录数据安全网关。

2.在菜单栏选择 “日志管理“>“审计日志列表” 进入审计列表页面。

3.选择需要审计的日志，单击“操作”列的“审计”按钮，进行审计。

4.在审计日志列表页面查看审计结果。

4.4 云密评专区-数字证书认证系统操作指南

4.4.1 CA 证书管理

CA 证书是一种数字证书，由认证机构（Certificate Authority，简称 CA）颁发，用于证明某一主体（如组织机构）的身份合法性，有时也被称为网络的身份证 。

新增自签 CA 证书

1.使用管理员账号登录数字证书认证系统。

2.在左侧导航栏选择“机构管理 > CA 证书管理”，进入“CA 证书管理”页面。

3.单击“新增按钮”，进入“新增 CA 证书”页面。

4.选择“自签 CA”，并且填写相关内容。

参数	参数说明
别名	证书的名称

参数	参数说明
密钥算法	选择证书的密钥算法类型，支持选择以下两种类型： - RSA - SM2
密钥长度	选择证书的密钥长度，根据选择的密钥算法会有不同的密钥长度： - RSA 支持：1024、2048、3072、4096 - SM2 支持：256
签名算法	选择根证书支持的签名算法，根据选择的密钥算法会有不同的签名算法： - RSA 支持：SHA256WithRSA、SHA384WithRSA、SHA512WithRSA、SHA256WithRSA/PSS、SHA384WithRSA/PSS、SHA512WithRSA/PSS - SM2 支持：SM3WithSM2
有效期	选择开始时间和结束时间
证书模版	选择证书模版
是否使用自定义主题	选择是否使用通用证书主题： - 是：填写对应项，系统自动拼接主题内容 - 否：填写指定格式的主题内容，例如如 C=CN,CN=TEST
名称	自动主题选择“是”才需要填写，更新的 CA 根证书名称，存储在证书中使用者的 CN。

参数	参数说明
国家	自动主题选择“是”才需要填写，从下拉列表中共选择一个国家
省份、城市、单位、部门	自动主题选择“是”才需要填写，一般填写使用者信息，存储在证书的 DN 项中 非必填项

5.填写完成后单击“提交”，即完成自签 CA 的导入。

导入 CA 证书

1.使用管理员账号登录数字证书认证系统。

2.在左侧导航栏选择“机构管理 > CA 证书管理”，进入“CA 证书管理”页面。

3.单击“新增按钮”，进入“新增 CA 证书”页面。

4.选择“导入证书”，并且填写相关内容。

参数	参数说明
导入私钥	根据您自身需要导入的证书有无私钥自行选择，若您不选择导入私钥，则需要先生成证书 CSR。
CA 私钥	若您选择导入私钥，则需要上传私钥。(只能上传 pem 编码的 PKCS8 私钥，且不超过 10kb)
CA 证书	上传 CA 证书。(只能上传 pem 编码的证书或证书链，且不超过 10kb)

参数	参数说明
别名	别名和证书请求文件中的别名保持一致。

5.单击“提交”，完成证书导入。

后续操作

更新证书：选择需要更新的证书，单击“操作”列的“更新”按钮，即可开始更新证书相关信息。

下载证书：选择需要下载的证书，单击“操作”列的“下载”按钮，即可下载证书信息

查看证书详情：选择需要查看详情的证书，单击“操作”列的“查看”按钮，即可查看证书详情。

启用/禁用证书：选择需要启用/禁用的证书，单击“操作”列的“启用/禁用”按钮，即可启用/禁用证书。

4.4.2 子 CA 管理

子 CA 证书是由根证书授权的次级证书颁发机构颁发的数字证书 。

新增子 CA 证书

1.使用管理员账号登录数字证书认证系统。

2.在左侧导航栏选择“机构管理 > 子 CA 管理”，进入“子 CA 管理”页面。

3.单击“新增”开始新增子 CA 证书。

4.单击“上传文件”上传证书文件并且选择所属的 CA 证书。

5.根据需求选择是否使用模板，选择完成后单击“提交”即可完成子 CA 证书的新增。

后续操作

下载子 CA 证书：选择需要下载的子 CA 证书，单击“操作”列的“下载”按钮，即可下载子 CA 证书信息。

注销子 CA 证书：选择需要注销的子 CA 证书，单击“操作”列的“注销”按钮，即可注销子 CA 证书信息。

4.4.3 CRL 管理

CRL 全称为 Certificate Revocation List，中文名称为证书吊销列表。CRL 里存储了被注销证书的序列号、注销时间和注销原因，同时，为保证 CRL 的有效性，CRL 携带了 CA 的签名。

CRL 管理列举 CRL 列表，CRL 按照签名算法不同，分为 RSA CRL 和 SM2 CRL。通过 CRL 管理可实现手动签发 CRL、下载 CRL、查看和查找功能。

配置 CRL

1.使用管理员账号登录数字证书认证系统。

2.在左侧导航栏选择“CRL 管理 > CRL 配置”，进入“CRL 配置”页面。

3.填写 CRL 配置相关参数。

参数	参数说明
自动启动	选择是，则立刻和每次服务启动时开启 CRL 定时发布任务；

参数	参数说明
	选择否，停止 CRL 定时发布任务。
类型	选择签发 CRL 的类型 - 全量：签发全量 CRL - 增量：签发增量 CRL - 全量&增量：两者都签发
生成周期	定时生成 CRL 的周期，以小时为单位，默认为 1 小时

4.单击“提交”完成 CRL 配置。

CRL 相关操作

生成 CRL：在“CRL 列表”页单击“生成”按钮即可生成 CRL。当前 CA 可以实现完全 CRL 和增量 CRL，根据系统设置的 CRL 生成策略，如果只选择完全 CRL，每次生成的 CRL 都会覆盖前一同类型 CRL，因此列表里只有一个 RSA 算法 CRL 和一个 SM2 算法 CRL；增量 CRL 会生成每年产生的证书注销列表，同一个年的会覆盖。

下载 CRL：选择需要下载的 CRL，单击“操作”列的“下载”按钮，即可下载 CRL。

4.4.4 证书管理

4.4.4.13 证书申请

证书申请分为两种：PKCS10 申请和 UKEY 申请。

PKCS10 申请是指使用 P10 请求文件的形式进行证书的申请；

UKEY 申请是将用户信息录入进行证书的申请。

申请 PKCS10 证书

1.登录数字证书认证系统。

2.在左侧导航栏选择“证书申请 > PKCS10 申请”，进入“PKCS10 申请”页。

3.选择证书模板，选择 CA 证书，填写证书有效期。

注意：

证书模板中公钥算法要与证书请求文件中公钥的算法一致

4.根据业务需求选择是否使用模板。

5.选择完成后单击“提交”即完成 PKCS10 证书申请。

UKEY 申请

1.登录数字证书认证系统。

2.在左侧导航栏选择“证书申请 > UKEY 申请”，进入“UKEY 申请”页。

3.选择所属的“CA”，并且选择“密钥算法”、“密钥长度”、“签名算法”和“有效期”。

4.选择“模板”并且填写相关信息。

5.填写完成后，单击“提交”并且在弹出的对话框中选择 UKEY 类型，并且将 UKEY 与您的设备连接后单击“确定”。

4.4.4.14 证书其他操作

您的数字证书在申请完成后可以进行如下操作：证书更新、证书注销、证书冻结、证书解冻、证书延期。

证书更新

证书更新操作就是注销原证书然后签发新的证书。只能对有效证书进行证书更新操作。

1.使用操作员账户登录数字证书认证系统。

2.在左侧导航栏选择“证书管理 > 证书更新申请”，进入“证书更新申请”页面。

3.选择需要更新的证书，单击“操作”列的“更新”按钮，即可开始更新。

4.在更新申请页填写证书的有效期和主题内容后单击“提交”。

说明

- 更新的证书是 PKCS10 证书直接下载使用即可；
- 更新的证书是 UKEY 证书，则需要同步连接 UKEY 设备进行更新。

证书注销

证书注销就是使证书永久失效。只能对有效证书进行证书注销操作

1.使用操作员账户登录数字证书认证系统。

2.在左侧导航栏选择“证书管理 > 证书注销申请”，进入“证书注销申请”页面。

3.选择需要更新的证书，单击“操作”列的“注销”按钮，即可开始注销。

证书冻结

证书冻结就是使证书暂时失效。只能对有效证书进行证书冻结操作。冻结后证书可通过解冻操作使证书恢复有效。

1.使用操作员账户登录数字证书认证系统。

2.在左侧导航栏选择“证书管理 > 证书冻结申请”，进入“证书冻结申请”页面。

3.选择需要冻结的证书，单击“操作”列的“冻结”按钮，待程序响应开始冻结。

证书解冻

证书解冻是证书冻结的逆操作，使冻结的证书恢复有效。

1.使用操作员账户登录数字证书认证系统。

2.在左侧导航栏选择“证书管理 > 证书解冻申请”，进入“证书解冻申请”页面。

3.选择需要冻结的证书，单击“操作”列的“解冻”按钮，待程序响应开始解冻。

证书延期

证书延期操作是对已有的证书有效期后延，延长证书的使用期限。

1.使用操作员账户登录数字证书认证系统。

2.在左侧导航栏选择“证书管理 > 证书延期申请”，进入“证书延期申请”页面。

3.选择需要延期的证书，单击“操作”列的“延期”按钮。

4.在弹出的对话框中选择延期后的到期时间，单击“确定”完成延期操作。

4.4.4.15 密钥恢复

按照 CA 标准规范要求，CA 需要提供加密证书密钥对恢复功能。安全的恢复加密密钥对到安全存储介质，例如 USBKey。

密钥恢复功能有密钥恢复申请和密钥恢复审核组成。其中，密钥恢复申请需要注册操作员权限，密钥恢复审核需要审核操作员权限。

注意：

密钥恢复暂不支持 ECDSA 算法。

恢复密钥操作步骤

1.使用操作员账户登录数字证书认证系统。

2.在左侧导航栏选择“密钥恢复 ”，根据您自身的需求选择“有效证书密钥恢复”、“过期证书密钥恢复”或“注销证书密钥恢复”。

3.进入对应的密钥恢复页面，选择需要恢复密钥的证书，单击“操作”列的“恢复”按钮。

4.根据弹窗提示插入 UKEY 设备，选择 UKEY 类型并输入口令，恢复成功后加密密钥将保存到 ukey 中。

5 最佳实践

5.1 如何使用综合安全网关保护设备的安全

网络和通信安全

身份鉴别和通信数据机密性、完整性

满足网络和通信安全的总体要求需要通过国密 SSL VPN 安全网关配合 VPN 客户端构建虚拟专用通道来保证对各通道的安全：

- 平台管理员通过 CN2 网络访问平台的业务通道：部署国密 SSL VPN 安全网关（配备数字证书），以及为平台管理员用户配备 USBKey（配备数字证书）和 VPN 客户端，建

立安全的国密加密通道，在此通道内访问平台；

- 平台运维人员通过 CN2 网络对平台的运维通道：部署国密 SSL VPN 安全网关（配备数字证书），以及为运维人员配备 USBKey（配备数字证书）和 VPN 客户端，建立安全的国密加密通道，在此通道内对平台中的各设备和服务器、操作系统等进行运维和管理。

网络边界访问控制

网络边界访问控制信息存储在国密 SSL VPN 安全网关中，完整性已得到保护。国密 SSL VPN 安全网关设备取得国家密码检测部门颁发的商用密码产品认证证书，通过国密 SSL VPN 安全网关自身机制实现访问控制信息的保护，该密码应用要求指标可复用商用密码产品检测结果。

设备与计算安全

概述

系统的设备和计算安全层面，主要涉及业务服务器、数据库服务器、网络设备、安全设备。因此采用合规的 SSL VPN 安全网关、服务器密码机、智能密码钥匙、数字证书实现各项商用密码技术功能。

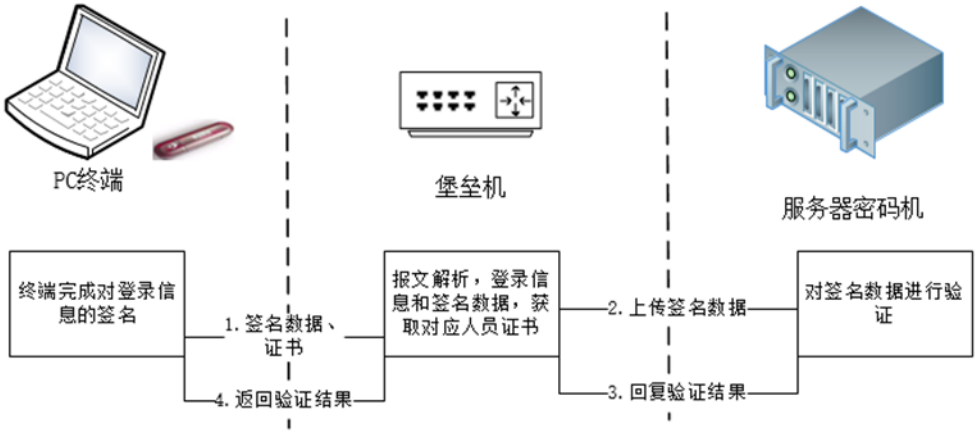
身份鉴别

通过专用 SSL VPN 安全网关结合运维堡垒机（或者 4A 安全系统）提供设备和计算层面的身份鉴别，结合智能密码钥匙（内置数字证书），运维人员 Ukey 数字证书由身份认证系统（CA）签发，并且与堡垒机分配给运维管理员的账户一一对应和绑定。

1.运维人员首先使用 VPN 客户端调用智能密码钥匙，通过远程（CN2 网络）连通合规 SSL

VPN 安全网关进行双向强身份认证，验证运维人员 USBKey 证书与 SSL VPN 服务的双方身份，握手成功后建立国密 SSL VPN 隧道。

2.再通过 UKey 方式登录堡垒机。用户通过智能密码钥匙登录堡垒机，采用挑战/应答机制，采用服务器密码机对登录签名进行验证，实现运维管理用户登录堡垒机的身份鉴别实现。具体过程如下：



- 用户插入智能密码钥匙访问堡垒机登录页面时，终端将签名数据、证书发送至堡垒机；
- 堡垒机将签名数据服务器密码机；
- 服务器密码机对签名数据进行验签，并返回验证结果至堡垒机；
- 堡垒机完成证书有消息验证，综合签名数据验证结果，将验证结果返回至终端。

基于密码技术的用户登录堡垒机的身份鉴别中，涉及的密钥为 SM2 签名算法公私钥，涉及的设备为智能密码钥匙和服务器密码机，不存在出现私钥明文情况。

3.通过堡垒机登录到服务器/虚机进行维护（SSH V2.0 协议），实现对服务器/虚机的管理和维护。

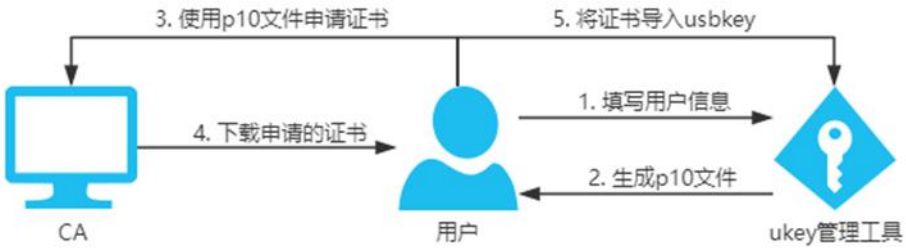
访问控制信息完整性

通过建立基于商用密码算法的 SSL VPN 安全通道，实现了对网络中的服务器、数据库、安全设备和密码设备等设备资产的集中管理。运维人员通过 SSL VPN 和堡垒机进行远程维护，首先用户使用 VPN 客户端登录 SSL VPN（运维通道），在运维终端和运维 SSL VPN 之间建立基于商用密码算法的 SSL VPN 集中管理通道，再通过堡垒机管理页面选择不同的管理协议和工具对设备进行管理，实现远程管理通道安全。

5.2 申请 PKCS10 证书并保存至 UKEY 中

概述

CA 提供使用 PKCS10 证书申请文件签发证书功能。用户可以使用 USBKey 管理员工具生成 PKCS10 文件，CA 将使用 PKCS10 中的用户信息和公钥签发证书。PKCS10 申请时支持使用证书模板，向签发的证书中添加扩展项和选择证书类型。CA 签发的证书可以使用 USBKey 管理员工具导入到 USBKey 中，完成业务闭环。

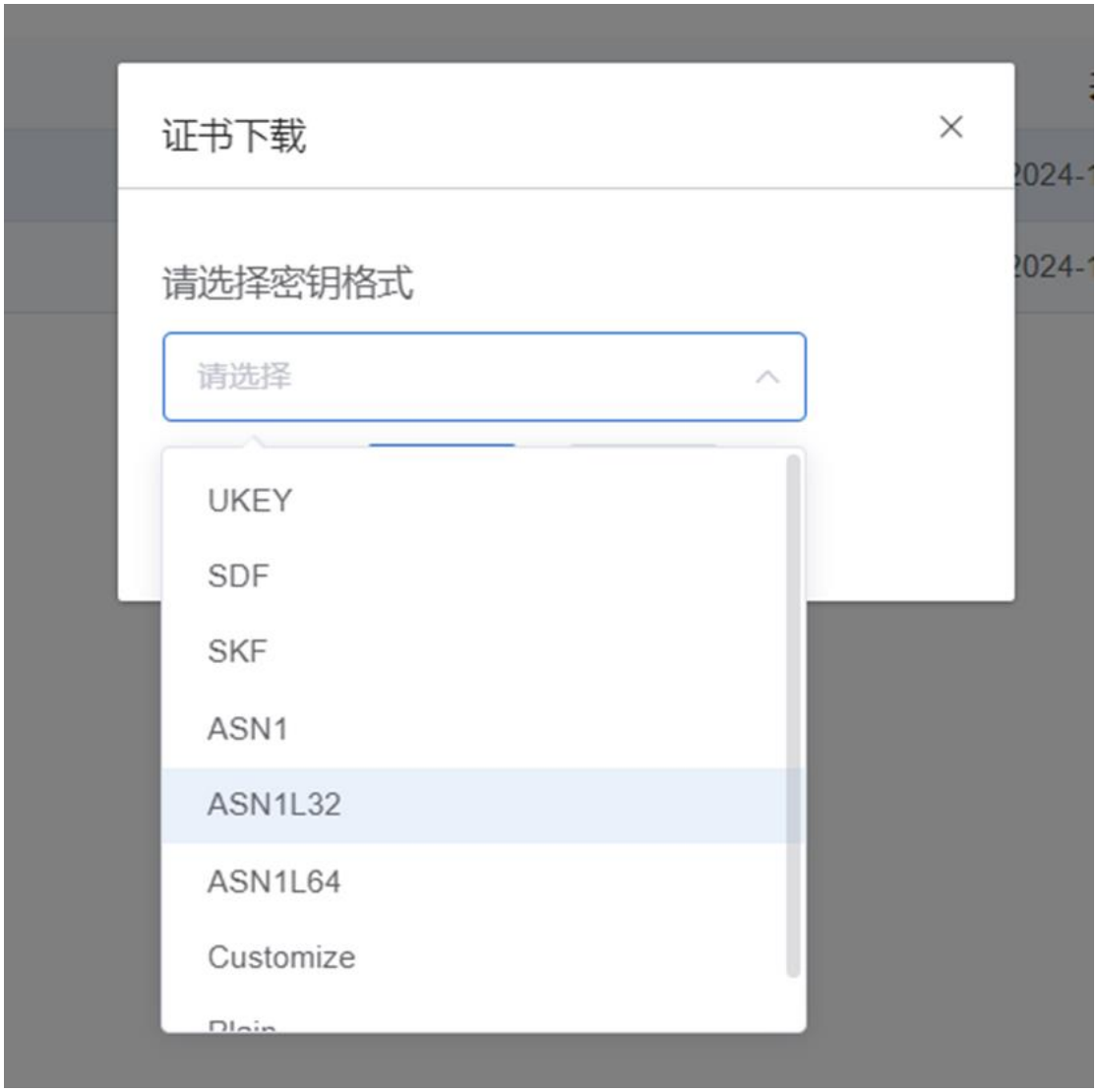


操作步骤

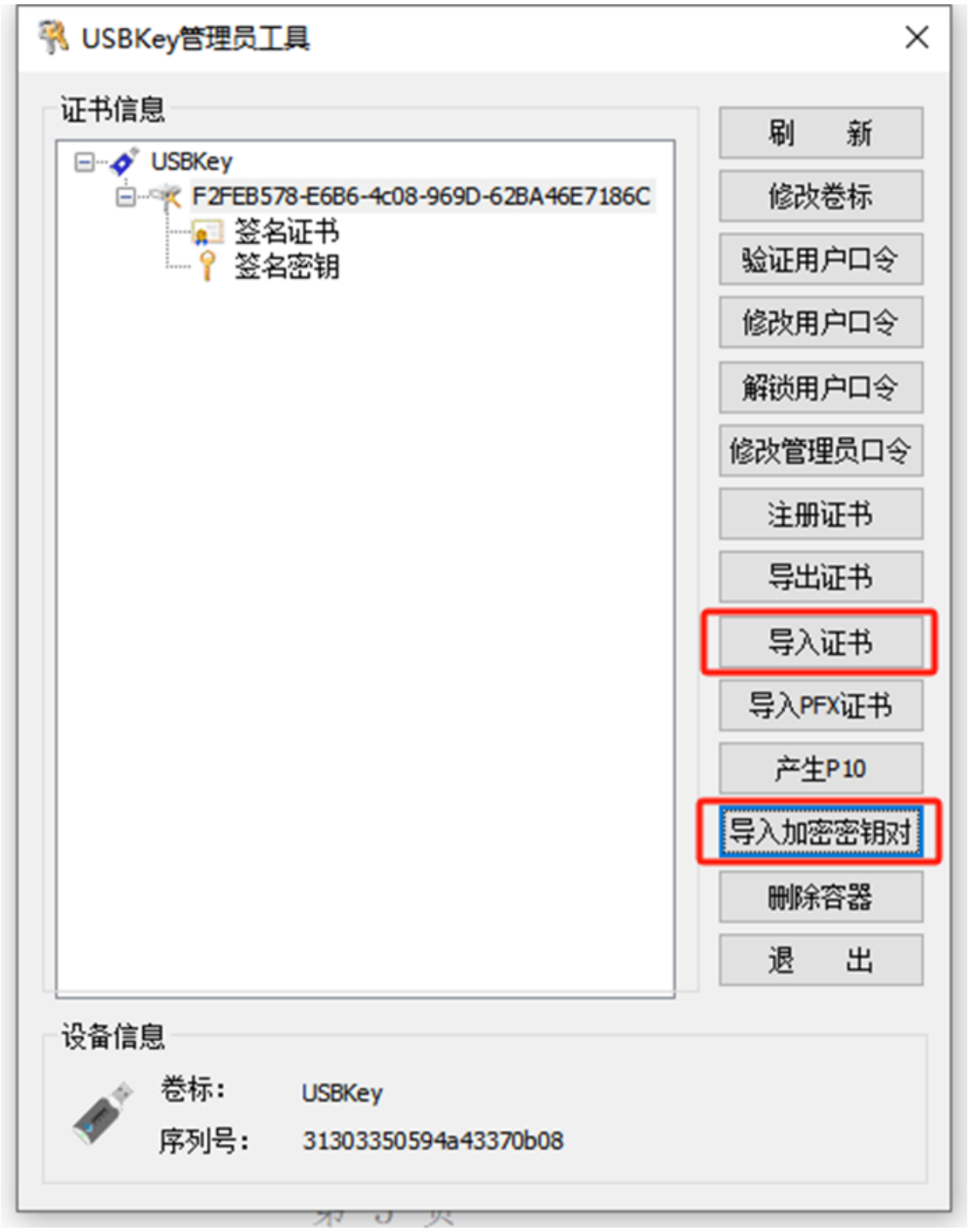
1.使用 USBKey 管理员工具生成 PKCS10 文件。

2.使用操作员账号登录 CA 管理页面，在“证书申请 > PKCS10 申请”中上传 PKCS10 文件，并选择 CA、模板等。

3.提交证书申请，申请成功后不要立即下载证书，在“证书下载 > 有效证书下载”中找到刚签发的证书，点击下载，选择不下载到 ukey，密钥格式选择 ASN1L32。



4.使用 USBKey 管理员工具，将下载的签名证书、加密证书和加密密钥分别使用导入证书、导入加密密钥对功能导入到 UKEY 中。


USBKey管理员工具
证书信息
USBKey
F2FEB578-E6B6-4c08-969D-62BA46E7186C
签名证书
签名密钥
刷　新
修改卷标
验证用户口令
修改用户口令
解锁用户口令
修改管理员口令
注册证书
导出证书
导入证书
导入PFX证书
产生P10
导入加密密钥对
删除容器
退　出
设备信息
卷标：
USBKey
序列号：
31303350594a43370b08

6 常见问题

6.1 产品咨询类

为什么要做密评?

- 开展密评，是为了解决商用密码应用中存在的突出问题，为网络和信息系统的安全提供科学评价方法，逐步规范商用密码的使用和管理。从根本上改变商用密码应用不广泛、不规范、不安全的现状，确保商用密码在网络和信息系统中有效使用，切实构建起坚实可靠的网络安全密码屏障。
- 《密码法》第二十七条：法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护，自行或者委托商用密码检测机构开展商用密码应用安全性评估。
- 《商用密码管理条例》第六章第三十八条：法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护，制定商用密码应用方案，配备必要的资金和专业人员，同步规划、同步建设、同步运行商用密码保障系统，自行或者委托商用密码检测机构开展商用密码应用安全性评估。
- 《商用密码应用安全性评估管理办法（试行）》第一章第三条：“涉及国家安全和社会公共利益的重要领域网络和信息系统的建设、使用、管理单位应当健全密码保障体系，实施商用密码应用安全性评估”。重要领域网络和信息系统包括：基础信息网络、涉及国计民生和基础信息资源的重要信息系统、重要工业控制系统、面向社

会服务的政务信息系统，以及关键信息基础设施、网络安全等级保护第三级及以上信息系统。

密评整体流程?

密评整体流程共包括 4 个阶段，分别为编写密码应用方案、密码应用方案评估、系统建设/改造、密码应用安全性评估。

- 编写密码应用方案：客户首先自行或委托密评机构按照密评标准对系统进行差距分析，根据差距分析结果结合系统实际情况设计密码应用方案，密码应用方案应包括系统现状及存在的风险、系统涵盖的重要数据、密码应用需求、方案设计以及使用的密码技术、管理制度、应急方案以及实施方案等。
- 密码应用方案评估：密码应用方案编写完成后，可委托密码专家或密评机构对密码应用方案进行评审，若委托密码专家对方案评审则出具专家评审意见，若委托密评机构评审，则出具密码应用方案评估报告。
- 系统建设/改造：密码应用方案通过评审后，系统集成单位按照通过评审的方案对系统进行建设或改造。
- 密码应用安全性评估：系统建设/改造完成后，被测单位委托密评机构对系统进行测评，密评机构按照 GB/T 39786 标准测评并出具差距分析报告，客户根据差距分析结果进行整改并申请复测，最终出具符合要求的商用密码应用安全性评估报告。

云密评专区的防护功能是否就能满足密评合规需求?

云密评专区可满足密评二级、三级的安全技术合规要求，密评第一级~第四级密码应用基本要求见下表。

- 对于“可”的条款，由信息系统责任单位自行决定是否纳入标准符合性测评范围。若纳入测评范围，则密评人员应按照相应的测评指标要求进行测评和结果判定；否则，该测评指标为“不适用”。
- 对于“宜”的条款，密评人员根据信息系统的密码应用方案和方案评审意见决定是否纳入标准符合性测评范围；若信息系统没有通过评估的密码应用方案或密码应用方案未做明确说明，则“宜”的条款默认纳入标准符合性测评范围。若纳入测评范围，则密评人员应按照测评指标要求进行测评和结果判定。否则，密评人员应根据信息系统的密码应用方案和方案评审意见，在测评中进一步核实密码应用方案中所描述的风险控制措施使用条件在实际的信息系统中是否被满足，且信息系统的实施情况与所描述的风险控制措施是否一致，若满足使用条件，该测评指标为“不适用”，并在密码应用安全性评估报告中体现核实过程和结果；若不满足使用条件，则应按照测评指标要求进行测评和结果判定。

- 对于“应”的条款，密评人员应按照测评指标要求进行测评和结果判定；若根据信息系统的密码应用方案和方案评审意见，判定信息系统确无与某项或某些项测评指标相关的密码应用需求，则相应测评指标为“不适用”。

表 A.1　第一级～第四级密码应用基本要求汇总列表

指标体系			第一级	第二级	第三级	第四级
技术要求	物理和环境安全	身份鉴别	可	宜	宜	应
		电子门禁记录数据存储完整性	可	可	宜	应
		视频监控记录数据存储完整性	—	—	宜	应
		密码服务	应	应	应	应
		密码产品	—	一级及以上	二级及以上	三级及以上
	网络和通信安全	身份鉴别	可	宜	应	应
		通信数据完整性	可	可	宜	应
		通信过程中重要数据的机密性	可	宜	应	应
		网络边界访问控制信息的完整性	可	可	宜	应
		安全接入认证	—	—	可	宜
		密码服务	应	应	应	应
		密码产品	—	一级及以上	二级及以上	三级及以上
	设备和计算安全	身份鉴别	可	宜	应	应
		远程管理通道安全	—	—	应	应
		系统资源访问控制信息完整性	可	可	宜	应
		重要信息资源安全标记完整性	—	—	宜	应
		日志记录完整性	可	可	宜	应
		重要可执行程序完整性、重要可执行程序来源真实性	—	—	宜	应
		密码服务	应	应	应	应
		密码产品	—	一级及以上	二级及以上	三级及以上
	应用和数据安全	身份鉴别	可	宜	应	应
		访问控制信息完整性	可	可	宜	应
		重要信息资源安全标记完整性	—	—	宜	应
		重要数据传输机密性	可	宜	应	应
		重要数据存储机密性	可	宜	应	应
		重要数据传输完整性	可	宜	宜	应
		重要数据存储完整性	可	宜	宜	应
		不可否认性	—	—	宜	应
		密码服务	应	应	应	应
		密码产品	—	一级及以上	二级及以上	三级及以上

指标体系			第一级	第二级	第三级	第四级
管理要求	管理制度	具备密码应用安全管理制度	应	应	应	应
		密钥管理规则	应	应	应	应
		建立操作规程	—	应	应	应
		定期修订安全管理制度	—	—	应	应
		明确管理制度发布流程	—	—	应	应
		制度执行过程记录留存	—	—	应	应
	人员管理	了解并遵守密码相关法律法规和密码管理制度	应	应	应	应
		建立密码应用岗位责任制度	—	应	应	应
		建立上岗人员培训制度	—	应	应	应
		定期进行安全岗位人员考核	—	—	应	应
		建立关键岗位人员保密制度和调离制度	应	应	应	应
	建设运行	制定密码应用方案	应	应	应	应
		制定密钥安全管理策略	应	应	应	应
		制定实施方案	应	应	应	应
		投入运行前进行密码应用安全性评估	可	宜	应	应
		定期开展密码应用安全性评估及攻防对抗演习	—	—	应	应
	应急处置	应急策略	可	应	应	应
		事件处置	—	—	应	应
		向有关主管部门上报处置情况	—	—	应	应

6.2 产品使用类

如何确定被测信息系统密码应用等级?

GB/T 39786-2021 中的密码应用等级一般由网络安全等级保护的级别确定。信息系统根据 GB/T 22240-2020《信息安全技术网络安全等级保护定级指南》确定等级保护级别时，同步对应确定密码应用等级，即等保定级为第一级的网络与信息系统应遵循 GB/T 39786-2021 第一级密码应用基本要求，等保定级为第二级的网络与信息系统应遵循 GB/T 39786-2021 第二级密码应用基本要求，以此类推。对于未完成网络安全等级保护定级的重要信息系统，其密码应用等级至少为第三级。因此在进行密码测评时，建议至少先完成等保的定级备案。

资源池没过密评，客户能部署云密评专区过密评，拿到测评报告吗?

云平台是否过密评不会直接影响租户侧的密评结果，若平台侧已经通过密评，那么云上租户在进行商用密码应用安全性评估时可复用平台侧的部分结果，如云平台已经进行了测评且拿到符合要求的密评报告，那么云上租户在进行测评时可复用物理和环境安全（即机房）的测评结果，反之，若平台侧没有通过密评，那么云上租户在进行密码测评时则不能复用平台侧的测评结果，需要按照密评标准 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》逐条测评。

购买了云密评专区是否还需要购买密码测评服务?

需要，云密评专区主要为客户提供密码改造服务，即根据客户的业务需求提供加解密、签名验签、SSL 加密服务等接口，协助客户按照密评标准满足身份鉴别、通道加密、重要数据存储等指标，需要由客户和云公司共同完成，而密码测评指的是系统建设/改造完成后委托密评机构按照密评标准 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》分别从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、管理制度、人员管理、建设运行和应急处置等多个维度对系统进行测评，由测评机构、客户和云公司共同完成，目前全国共有 48 家密评机构可进行全国系统的测评。

应用系统是否涉及代码改造?

客户在购买了云密评专区后还需要对应用系统进行代码改造才能满足业务系统的密码需求，客户通过业务系统实际需求调用云密评专区对应的服务，如身份鉴别不满足需求，则需要调用身份认证服务对应的接口，如未对重要业务数据进行安全存储，则根据实际需求，若重要数据需要进行防泄漏（机密性）保护，则调用加解密服务接口以保证重要业务数据的存储机密性，若重要数据需要进行防篡改（完整性）保护，则调用签名验签及服务接口保证重要数据的存储完整性。云密评专区可提供的服务见下表。

密码服务	服务说明
加解密服务	为应用系统提供重要数据的加密和解密服务，满足密评中对重要数据传输和存储的机密性要求。
身份认证服务	为应用系统提供对登录用户的基于国密数字证书的身份认证服务，保证应用系统用户身份的真实性，满足密评中对用户身份真实性鉴别的要求。
签名验签服务	为应用系统提供重要数据的签名和验签服务，满足密评中对重要数据传输和存储的完整性要求以及操作的不可否认性要求。
密钥管理服务	为应用系统提供集中的密钥全生命周期管理服务，满足密评中对密钥管理的安全性要求。
杂凑密码服务	为应用系统提供杂凑密码运算服务，满足密评中对重要数据传输和存储的完整性要求。
数字证书服务	为用户、应用或设备提供数字证书的签发、更新、注销等全生命周期的管理，为身份鉴别提供数字证书支撑服务。
SSL 加密服务	提供网络通信通道的加密服务，满足密评中对网络和通信安全层面的数据传输机密性和完整性要求。
电子签章服务	为应用系统提供电子签章服务，电子签章以数字证书为基础，将数字签名、印章图片以及被签章对象进行结合，通过签章形式，满足不可否认性要求。

密码服务	服务说明
协同签名服务	配合移动端密码模块为应用系统移动端提供协同密码服务，满足移动端的密码应用合规性要求。
时间戳服务	为应用系统提供用于证明原发数据的产生时间，满足时间不可否认性的要求。

SSL VPN 网关是什么？

SSL VPN 网关是专为解决网络间安全互联设计的一款高性能安全产品，基于 SSL 协议为应用提供基于数字证书的高强度身份认证服务、高强度数据透明隧道加密服务，可以有效保护网络资源的安全访问。

数据加密网关是什么？

数据加密网关针对于数据库数据存储安全的高性能密码网关设备，是基于数据库透明加密原理的数据库主动防御产品，具有透明加解密及完整性保护、密钥合规生命周期管理、独立于数据库的权限控制等功能特性。

数据加密网关与通用服务器密码机的区别？

通用服务器密码机	数据库加密网关
使用通用服务器密码机对代码进行改造实现对数据库数据加密	使用专用数据库加密网关进行应用集成实现数据库中数据透明加密
加密能力深入应用代码，用户自主性高	应用系统无需进行代码改造，应用集成数据库加密机即可完成数据库的加密改造，数据自动被加密和解密；
应用需进行代码改造，用户、应用开发商、密码机厂商以及测评机构需要紧密配合；应用需要解决加密改造中碰到的技术难题（模糊查询等）。	某些加密模式需要改变应用和数据库的网络拓扑结构。