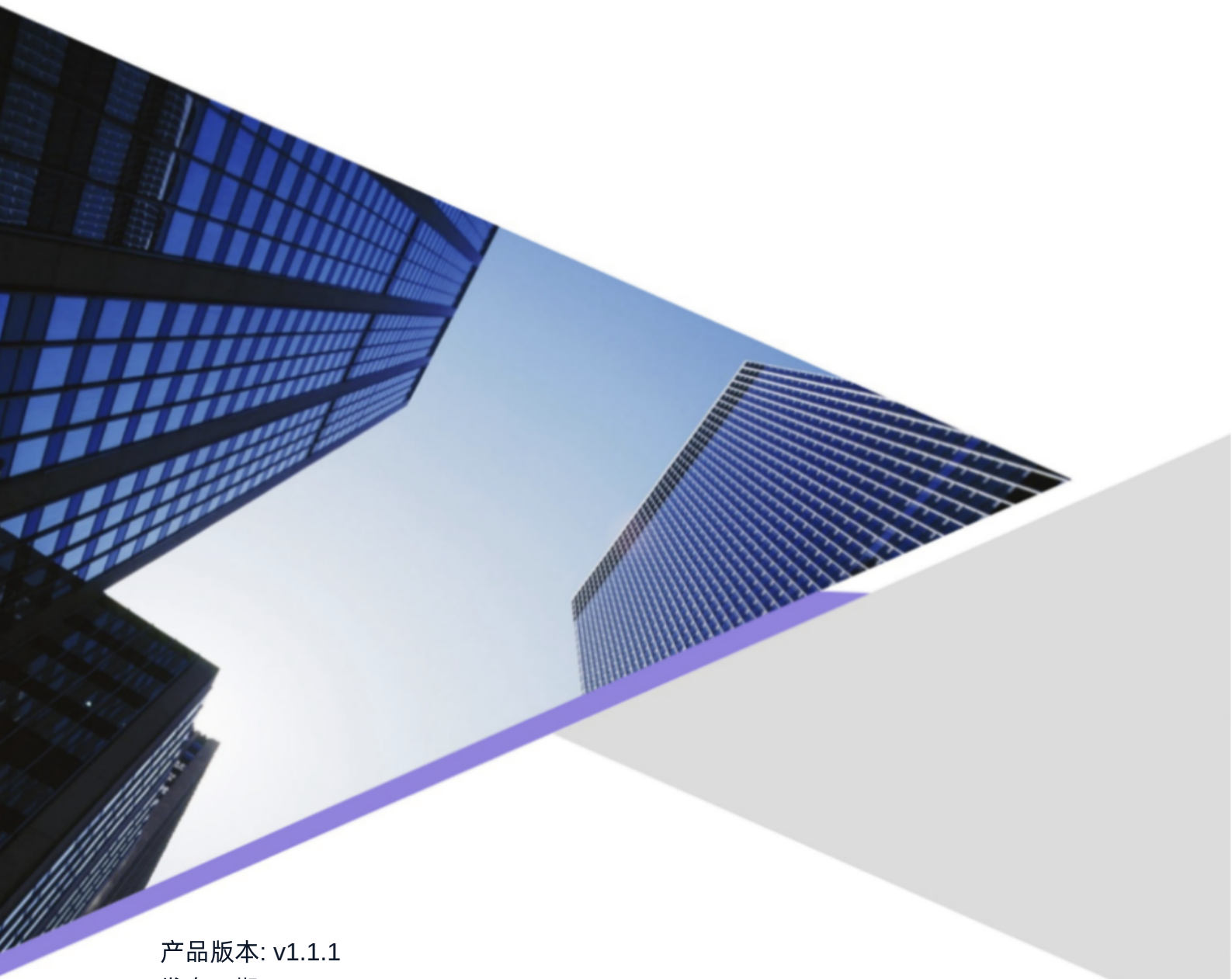
易捷行云
EasyStack

证书与密钥服务

快速入门



产品版本: v1.1.1
发布日期: 2023-06-20

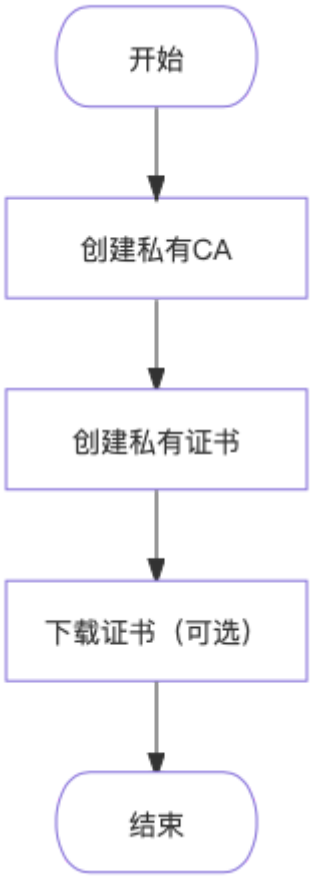
目录

1 快速入门

1.1 证书服务

1.1.1 操作指引

证书服务的主线使用流程及具体说明如下：



操作流程	描述
创建私有CA	创建证书时需选择由哪个私有CA签发。若所需私有CA已存在，可跳过此步直接创建证书。

操作流程	描述
创建私有证书	确认签发CA存在后，即可创建私有证书。
下载证书（可选）	证书创建完成后，可根据证书使用场景选择是否下载证书分发给用户安装使用。

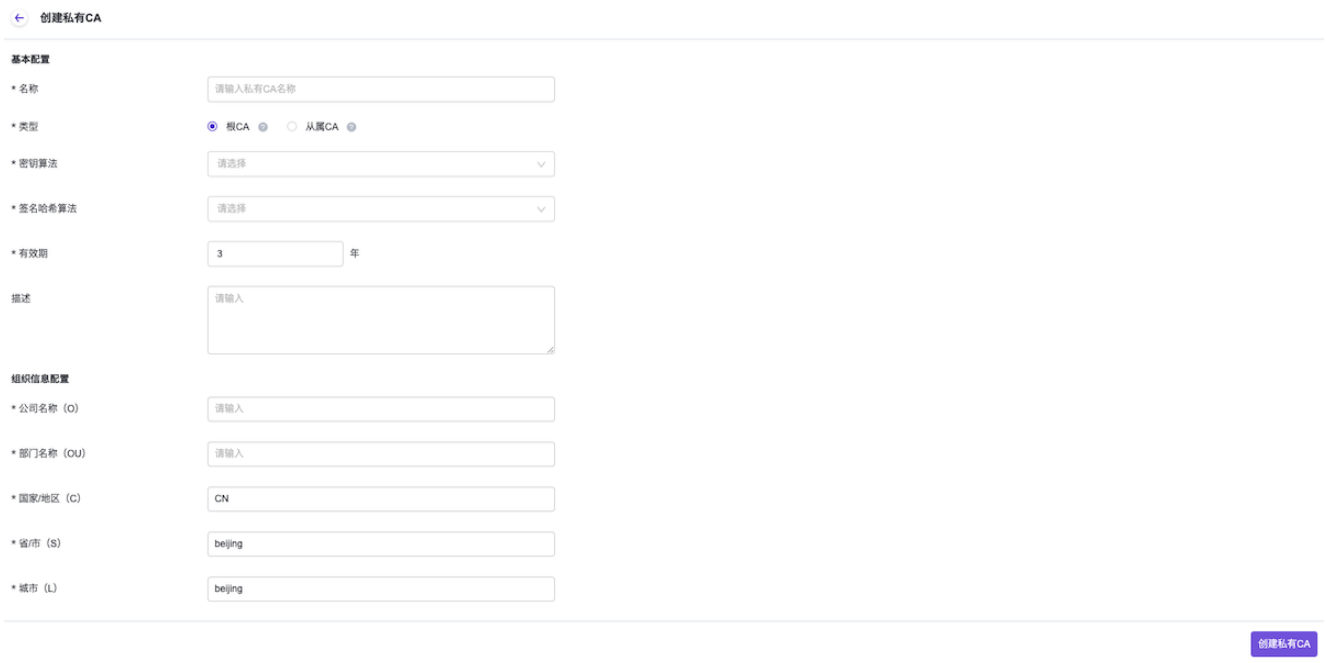
1.1.2 创建私有CA

> 说明：
> - 项目中首次创建私有CA时只能创建根CA。后续可选择创建根CA或从属CA。
> - 私有CA创建完成后默认为“已启用”状态。

1. 在顶部导航栏中，依次选择[产品与服务]-[证书与密钥服务]-[私有CA]，进入“私有CA”页面。

2. 单击 `创建私有CA` ，进入“创建私有CA”页面。

3. 配置参数后，单击 `创建私有CA` ，完成操作。



参数	说明
类型	私有CA分为根CA和从属CA，根CA下可以包含多个从属CA，每个从属CA下可以包含多个下一级的从属CA，从而形成一套CA层次结构。但对于每套CA层次结构，只有最顶层的CA被称为根CA。因此，若要建立新的CA层次结构，可选择“根CA”；若要在现有CA层次结构中增加新的成员，可选择“从属CA”。
签发CA	仅当“类型”选择“从属CA”时显示，选择该从属CA由哪一私有CA签发。

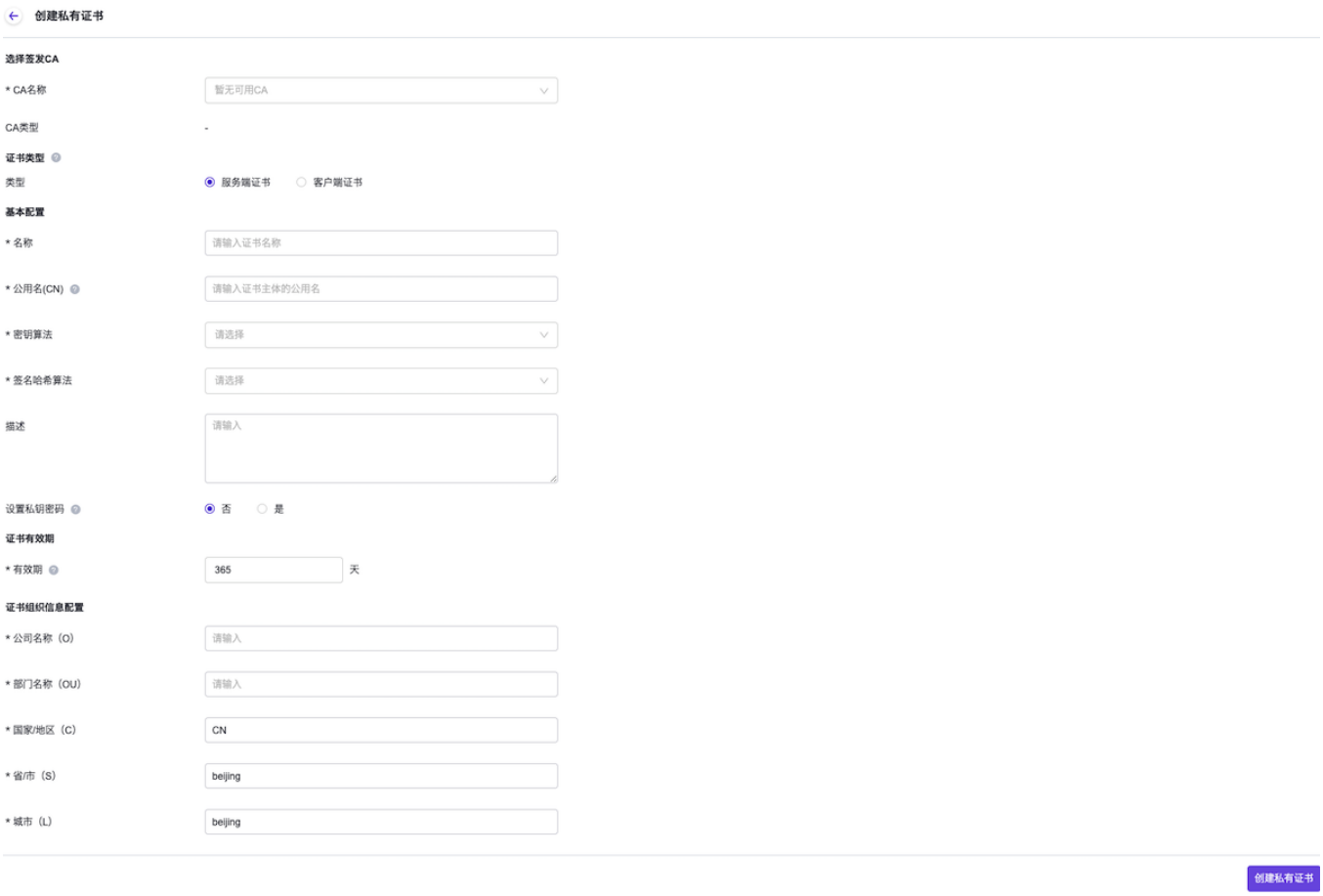
参数	说明
密钥算法	选择私有CA签发证书时所使用的加密算法类型。当前支持RSA2048、RSA4096、ECC256、ECC384、国密SM2。对于从属CA，若其签发CA使用的是国密SM2算法，则从属CA只能使用相同算法。
签名哈希算法	选择私有CA签发证书时所使用的哈希算法类型。当前支持SHA256、SHA384、SHA512、国密SM3。当且仅当“密钥算法”参数选择了“国密SM2”时，本参数可选择“国密SM3”。
有效期	根CA有效期的取值范围为3至30年。从属CA有效期的取值范围为1至20年，同时，不能超过其签发CA的剩余有效期。有效期不足1年时，无法签发从属CA。有效期结束后私有CA将变为“已过期”状态，无法继续签发证书，且该私有CA曾经签发过的证书也将失效。
路径深度	路径深度决定了该CA可以继续签发下级从属CA的层级，可填写的最小值为0，最大值=其签发CA的路径深度-1。签发CA的路径深度可在其详情页的“基本信息”区域查看。根CA的默认路径深度为7。路径深度为0的私有CA无法继续签发从属CA（签发私有证书不受影响）。例如，某一根CA名称为a，现创建一个由a直接签发的从属CA，名称为b，则b的路径深度可设置的范围为0～6（左右包含）中的整数。假设b的路径深度设置为6，则由b签发的证书链中深度最大的一条可能的情况是：b->c->d->e->f->g->h。
公司名称	根据申请单位实际情况填写即可。
部门名称	
国家/地区	
省/市	
城市	

1.1.3 创建私有证书

创建证书时将自动生成证书文件及私钥。

> 说明：
> 创建完成后，除描述外其它信息均不支持修改。

1. 在顶部导航栏中，依次选择[产品与服务]-[证书与密钥服务]-[证书管理]，进入“证书管理”页面。
2. 单击 `创建私有证书` ，进入“创建私有证书”页面。
3. 配置参数后，单击 `创建私有证书` 完成操作。



参数		说明
选择签发CA	CA名称（CN）	选择签发该证书的CA。

参数		说明
	类型	签发该证书的CA的类型，包括根CA和从属CA，根据所选CA自动显示，无需配置。
证书类型	类型	证书类型分为服务端证书和客户端证书。服务端证书安装到应用的服务器端，用于证明站点所有者身份；客户端证书安装到访问应用的客户端软件，用于验证客户端身份。
基本配置	名称	私有证书的名称。
	公用名（CN）	私有证书主体的通用名称。 * 服务端证书通常填写服务域名，如果未指定域名，那么在使用生成的服务端证书配置HTTPS服务后，浏览器访问服务时可能提示“此站点不安全”等。域名支持以“*”开头的泛域名。 * 客户端证书通常填写用户邮箱地址或者用户名等可以标识客户端身份的信息。
	密钥算法	证书使用的密钥算法和密钥的位大小，当前支持RSA2048、RSA4096、EC256、EC384、国密SM2。若签发CA使用的密钥算法为“国密SM2”，则本参数只能使用相同算法。若签发CA使用的密钥算法非“国密SM2”，则本参数不支持选择“国密SM2”。
	签名哈希算法	证书使用的签名哈希算法，当前支持SHA256、SHA384、SHA512、国密SM3。当且仅当“密钥算法”参数选择了“国密SM2”时，本参数可选择“国密SM3”。
	设置私钥密码	私钥密码用于对证书私钥进行加密，目前不支持密码找回功能，请牢记私钥密码，后续安装私有证书时，需要使用此处密码对私钥解密。
证书有效期	有效期	证书有效期应小于其签发CA的剩余有效期，且上限为7300天。若签发CA剩余有效期不足1天，则无法签发证书。有效期结束证书即失效，访问使用该证书的应用时，将提示证书已过期。
证书组织信息配置	公司名称	根据证书隶属组织实际情况填写即可。
	部门名称	

参数		说明
	国家/地区	
	省/市	
	城市	

1.1.4 下载证书（可选）

下载证书分发给用户安装使用。

1. 在顶部导航栏选择[产品与服务]-[证书与密钥服务]-[证书管理]，进入“证书管理”页面。

2. 单击目标证书操作栏的 `下载` ，弹出“下载证书”对话框。

3. 不同密钥算法的证书下载方式及文件格式如下：

   - 使用RSA和ECC密钥算法的证书：选择服务器类型，单击 `下载` 完成操作。
   - 使用国密算法的证书：直接单击 `下载` 完成操作。国密证书目前仅支持下载通用格式的证书文件，包含签名证书和加密证书双证书，详细说明见下方表格。

使用RSA和ECC密钥算法的证书文件说明：

证书类型	服务器类型	证书压缩包中的文件	文件说明
服务端证书	Tomcat	server.jks	Java KeyStore格式的证书文件。
		keystorePass.txt	加密证书的密码。
	Nginx	server.crt	证书文件。
		server.key	证书对应的私钥文件。
		chain.crt	该证书的签发CA到根CA的CA证书链文件。
	Apache	server.crt	证书文件。
		server.key	证书对应的私钥文件。
		chain.crt	该证书的签发CA到根CA的CA证书链文件。
	IIS	server.pfx	PKCS#12格式的证书文件。

证书类型	服务器类型	证书压缩包中的文件	文件说明
		keystorePass.txt	加密证书的密码。
	其他	server.pem	证书文件。
		server.key	证书对应的私钥文件。
		chain.pem	该证书的签发CA到根CA的CA证书链文件。
客户端证书	Tomcat	client.crt	证书文件，按需配置到客户端中即可。
		client.key	证书对应的私钥文件，按需配置到客户端中即可。
		client.pfx	证书和私钥合并后的PKCS#12证书文件(证书未加密)，按需配置到客户端中即可。使用合并的证书文件与使用单独的证书&私钥文件两种方式二选一即可。
		client- ca.truststore	证书签发CA的Truststore文件，需配置到Tomcat服务配置文件中的 **truststoreFile** 处。
		keystorePass.txt	加密client-ca.truststore文件的密码，需配置到Tomcat服务配置文件中的 **truststorePass** 处。
	Nginx	client.crt	证书文件，按需配置到客户端中即可。
		client.key	证书对应的私钥文件，按需配置到客户端中即可。
		client.pfx	证书和私钥合并后的PKCS#12证书文件(证书未加密)，按需配置到客户端中即可。使用合并的证书文件与使用单独的证书&私钥文件两种方式二选一即可。

证书类型	服务器类型	证书压缩包中的文件	文件说明
		client-ca.pem	证书的签发CA到根CA的CA证书链文件，需配置到Nginx服务配置文件中 **ssl_client_certificate** 处，并开启 **ssl_verify_client on** 配置。
	Apache	client.crt	证书文件，按需配置到客户端中即可。
		client.key	证书对应的私钥文件，按需配置到客户端中即可。
		client.pfx	证书和私钥合并后的PKCS#12证书文件(证书未加密)，按需配置到客户端中即可。使用合并的证书文件与使用单独的证书&私钥文件两种方式二选一即可。
		client-ca.pem	证书的签发CA到根CA的CA证书链文件，需配置到Apache Httpd服务配置文件中 **SSLCACertificateFile** 处，并开启 **SSLVerifyClient require** 配置。
	IIS	client.crt	证书文件，按需配置到客户端中即可。
		client.key	证书对应的私钥文件，按需配置到客户端中即可。
		client.pfx	证书和私钥合并后的PKCS#12证书文件(证书未加密)，按需配置到客户端中即可。使用合并的证书文件与使用单独的证书&私钥文件两种方式二选一即可。
		client-ca.pem	证书的签发CA到根CA的CA证书链文件，需将证书链文件中的每一个证书导入到部署IIS服务的Windows系统的“受信任的证书颁发机构”当中。
	其他	client.crt	证书文件，按需配置到客户端中即可。

证书类型	服务器类型	证书压缩包中的文件	文件说明
		client.key	证书对应的私钥文件，按需配置到客户端中即可。
		client.pfx	证书和私钥合并后的PKCS#12证书文件(证书未加密)，按需配置到客户端中即可。使用合并的证书文件与使用单独的证书&私钥文件两种方式二选一即可。
		client-ca.pem	证书的签发CA到根CA的CA证书链文件，需配置到指定服务的客户端证书认证配置项中。

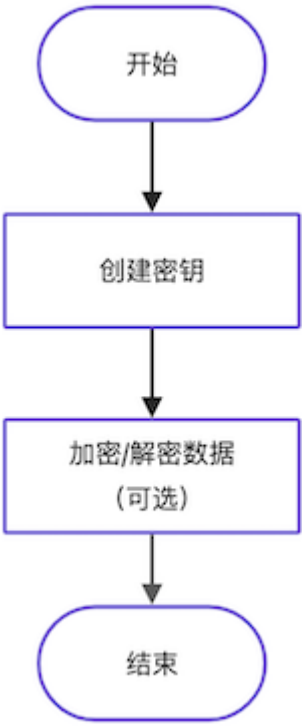
使用国密密钥算法的证书文件说明：

证书类型	证书压缩包中的文件	文件说明
服务端证书	server_sig_cert.pem	签名证书
	server_sig_key.pem	签名证书对应的私钥文件
	server_enc_cert.pem	加密证书
	server_enc_key.pem	加密证书对应的私钥文件
	chain.pem	证书的签发CA到根CA的CA证书链文件
客户端证书	client_sig_cert.pem	签名证书
	client_sig_key.pem	签名证书对应的私钥文件
	client_enc_cert.pem	加密证书
	client_enc_key.pem	加密证书对应的私钥文件
	chain.pem	证书的签发CA到根CA的CA证书链文件

1.2 密钥服务

1.2.1 操作指引

密钥服务的主线使用流程及具体说明如下：



操作流程	描述
创建密钥	依据客户实际业务需求，创建对应类型的密钥。即当加解密需要使用相同的密钥时，请创建对称密钥，否则请创建非对称密钥。
加密/解密数据（可选）	当所创建密钥的类型为对称密钥时，可以在云平台中通过在线工具，对数据执行加密或解密操作。

1.2.2 创建密钥

本操作用于在云平台中依据客户实际业务需求，创建对应类型的密钥。即当加解密需要使用相同的密钥时，请创建对称密钥，否则请创建非对称密钥。

1. 在顶部导航栏中，依次选择[产品与服务]-[证书与密钥服务]-[密钥管理]，进入“密钥管理”页面。

2. 单击 `创建密钥` ，弹出“创建密钥”对话框。

3. 配置参数后，单击 `确认` ，完成操作。

参数	说明
名称	该密钥的名称。
保护级别	该密钥的保护级别。该参数值可选Software或HSM。 * Software：通过软件密码模块对密钥进行保护。 * HSM：Hardware Security Module（硬件安全模块），通过专用硬件对密钥进行高安全等级保护，即密钥的产生和运算都在加密机中进行。
密钥算法	该密钥的算法。 * 当“保护级别”选择“Software”时，该参数值可以选择“AES_256”（对称密钥），用于加密解密，也可以选择“ RSA_2048”（非对称密钥），用于签名验签。 * 当“保护级别”选择“HSM”时，密钥算法和用途将依赖加密机动态获取。
密钥类型（不可编辑）	该密钥的类型。 该参数值会根据所选的密钥算法，自动配置为“对称密钥”或“非对称密钥”，而无需手动配置，且也不支持编辑。
密钥用途	该密钥的用途。 该参数值可选“encrypt_decrypt”，即加密解密，或“sign_verify”，即签名验签。
描述（可选）	该密钥的描述信息。

1.2.3 加密/解密数据（可选）

当所创建密钥的类型为对称密钥时，可以通过本操作在云平台中使用在线工具，对数据执行加密或解密操作。

1. 在顶部导航栏中，依次选择[产品与服务]-[证书与密钥服务]-[密钥管理]，进入“密钥管理”页面。

2. 单击密钥名称链接，进入该密钥详情页面。

3. 在“在线工具”区域框中，选择 [加密] 或 [解密] 页签。

4. 在左侧输入框中对应输入明文或密文后，单击 `执行` ，可在右侧显示框中查看到加/解密后的数据。

   单击 `复制到剪切板` ，可直接复制显示框中的加/解密后数据到剪切板中。

咨询热线：400-100-3070

北京易捷思达科技发展有限公司：
北京市海淀区西北旺东路10号院东区1号楼1层107-2号
南京易捷思达软件科技有限公司：
江苏省南京市雨花台区软件大道168号润和创智中心4栋109-110

邮箱：
contact@easystack.cn (业务咨询)
partners@easystack.cn(合作伙伴咨询)
marketing@easystack.cn (市场合作)