云执钥®远程可靠电子签名服务策略

(UniTrust Remote Reliable Electronic Signature Service Policy, RSP)

版本号 v1.0

生效日期：2026 年 10 月 31 日

上海市数字证书认证中心有限公司

上海市四川北路 1717 号 18 楼

《云执钥®远程可靠电子签名服务策略》为公开文件，归上海市数字证书认证中心有限公司所有。未经版权持有方书面许可，不得复制本文件的任何部分。

版本控制

版本	发布日期	发布者
V1.0　(现行版本)	2026 年 10 月 31 日	SHECA 安全认证委员会

变更摘要

版本	更新描述
V1.0	根据《T/CQAE 11034-2025：电子认证业务规则规范》要求，首次制订发布本 RSP。

目录

1. 引言 7

1.1 概述 7

1.2 文档与策略标识 7

1.3 策略管理 8

1.4 规范性引用文件 8

1.5 定义与缩略语 8

1.6 服务使用 11

1.6.1 适当服务使用 11

1.6.2 禁止的服务使用 11

1.7 法律与合规框架 11

1.7.1 适用法律法规 11

1.7.2 《信息安全等级保护管理办法》合规性声明 12

1.7.3 可靠电子签名保障措施 12

1.7.4 法律效力声明 13

2. 服务参与者 13

3. 身份鉴别与电子签名认证证书 13

3.1. 初始申请密钥的身份鉴别 13

3.1.1. 个人身份的鉴别 14

3.1.2. 机构身份的鉴别 14

3.2. 证书续期的身份鉴别 14

3.3. 证书变更的身份鉴别 14

4. 签名密钥生命周期管理 14

4.1. 密钥初始化 14

4.1.1. 密钥生成 14
4.1.2. 身份链接 15
4.1.3. 一次性签名密钥 15
4.2. 私钥交付 16
4.3. 签名激活 16
4.3.1. 基础级签名激活 16
4.3.2. 高等级签名激活 16
4.3.3. 解除私钥激活状态 16
4.4. 私钥销毁 16
4.5. 私钥备份与恢复 17
4.6. 会话密钥封装与恢复 17
4.7. 私钥归档 18
4.8. 私钥导入、导出 18
5. 设施、管理和操作控制 18
5.1. 物理安全控制 18
5.2. 程序控制 18
5.2.1. 可信角色 18
5.2.2. 需要职责分离的角色 19
5.3. 人员控制 19
5.4. 审计日志记录程序 19
5.5. 记录归档 19
5.6. 损害与灾难恢复 20
5.7. 服务可用性 20

5.8. 服务终止 20
6. 技术安全控制 20
6.1. 密码学、私钥及其保护 20
6.1.1. 密码算法 20
6.1.2. 私钥生成与保护 21
6.1.3. 私钥多人控制 21
6.1.4. 私钥销毁 21
6.1.5. 私钥备份与恢复 21
6.1.6. 远程电子签名安全保障 21
6.2. 计算机安全控制 22
6.3. 生命周期安全控制 22
6.4. 网络安全控制 23
7. 合规审计和其他评估 23
7.1. 评估频率或情形 23
7.2. 评估者的身份/资格 23
7.3. 评估者与被评估者的关系 23
7.4. 评估内容 23
7.5. 对问题与不足采取的措施 24
7.6. 评估结果的传达与发布 24
8. 法律责任和其他业务条款 24
8.1. 费用 24
8.2. 财务责任 24
8.3. 业务信息的保密 24

8.4. 个人信息的隐私 24
8.5. 知识产权 24
8.6. 声明与保证 25
8.6.1. 服务机构的声明与保证 25
8.6.2. 其他参与方的声明与保证 25
8.7. 担保免责 25
8.8. 责任限制 25
8.9. 赔偿 25
8.10. 有效期与终止 25
8.11. 对参与者的个别通告与沟通 25
8.12. 修订和发布 26
8.13. 争议处理与举证 26
8.14. 管辖法律 26
8.15. 与适用法律的符合性 26
8.16. 一般条款 26
8.17. 其他条款 26

1. 引言

1.1 概述

本文件由上海市数字证书认证中心有限公司（简称 SHECA）编制，规定了其在提供云执钥®可靠云签名时所遵循的政策和安全管理要求，并描述远程创建可靠电子签名方面所采取的行动。

该服务核心功能为基于 SHECA 签发的电子签名认证证书提供远程电子签名服务，用于签名操作的证书私钥全程在 SHECA 完全管控的密钥设备中生成并加密存储，只有经过订户授权才能使用。

本服务面向所有需要为创建电子签名的客户开放。SHECA 未对潜在最终用户设置准入限制，服务提供遵循非歧视性原则。

1.2 文档与策略标识

文档名称：云执钥®远程可靠电子签名服务策略

版本号：1.0

支持的策略 OID：

- 1.2.156.112570.50.1.1（Qualified RQESSS policy，QRSP）– 基础级远程可靠电子签名服务策略
- 1.2.156.112570.50.1.2（Enhanced RQESSS policy，ERSP）– 高等级远程可靠电子签名服务策略

使用方可根据业务风险等级和签名法律效力需求选择上述两种服务策略等级。两种等级的核心差异对比如下：

类别	QRSP（Qualified RQESSS policy）	ERSP（Enhanced RQESSS policy）
适用场景	适用于除 ERSP 规定场景外的其他电子签名场景	适用于涉及生命健康、财产权益等高风险场景
身份鉴别	符合 T/CQAE 11034-2025《电子认证业务规则规范》基础级证书要求	符合 T/CQAE 11034-2025《电子认证业务规则规范》高等级证书要求
证书类型	个人/机构基础级电子签名认证证书	个人/机构高等级电子签名认证证书
密钥生成设备	符合 GM/T 0028 安全二级以上经检测认证合格的硬件密码模块	

密钥存储设备	经符合 GM/T 0028 安全二级以上经检测认证合格的硬件密码模块加密后存储在防篡改可信执行环境的密钥库中

1.3 策略管理

本服务策略由 SHECA 安全认证委员会管理，负责策略的制定、批准、维护和解释。

联系人：SHECA 安全认证委员会

联系电话：86-21-36393197

联系邮箱：policy@sheca.com

联系地址：中华人民共和国上海市四川北路 1717 号嘉杰国际广场 18 楼，200080

批准程序：由基础产品部起草，经部门总监审核后，报 SHECA 安全认证委员会批准发布。

修订程序：如果因为标、技术、安全机制、运营环境和法律法规要求等重大变化，由基础产品部提交修改建议。修订稿经 SHECA 安全认证委员会批准后，更新版本并在 SHECA 网站（https://www.sheca.com）公布。

1.4 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 31508 信息安全技术 公钥基础设施 数字证书策略分类分级规范

GB/T 26855 信息安全技术 公钥基础设施 证书策略与认证业务声明框架

GM/T 0028 密码模块安全技术要求

GM/T 0009 SM2 密码算法使用规范

GM/Z 0001—2013 密码术语

T/CQAE 11034-2025 电子认证业务规则规范

1.5 定义与缩略语

术语	解释
远程可靠电子签名	经订户单独同意，由 SHECA 生成并保管但受订户唯一控制的私钥所生成的符合《电子签名法》第十三条所规定的条件的电子签名。
签名激活数据	用于使密码模块中的私钥进入可操作状态的数据，可以是口令、生物特征等。 来源：GB/T 31508—2015,3.13，有修改
密码模块	实现密码运算功能的、相对独立的软件、硬件、固件或其组合。 来源：GM/Z 4001—2013,2.53
待签名数据	是签名人签署的原始数据对象(如一份合同 PDF、一条 JSON 记录)，尚未经过任何签名标准格式化处理。
待签名格式化数据	将待签名数据（DTBS）按照相应签名标准（如 CAdES/XAdES/PAdES/JAdES）的规则进行格式化并置放于正确顺序而创建的数据，用于计算待签名数据表示。
待签名数据表示	是对待签名格式化数据（DTBSF）应用密码学哈希（Hash）算法后得到的哈希值（或称为消息摘要），用于计算数字签名值。
订户	被颁发给一张证书的证书主体。 来源：GB/T 26855—2011,3.15
证书主体	证书中的主体（subject）字段指明的、持有与证书中所载公钥相对应私钥的实体，亦称为证书持有人。当订户是法人机构时，证书主体还可以是该法人机构的下属机构、下属职员等。 来源：GB/T 31508—2015,3.6，有修改
证书申请人	向认证机构申请证书的自然人、法人或非法人组织。证书申请成功后，证书申请人即为订户。 来源：GB/T 31508—2015,3.7，有修改

电子签名人	是指持有电子签名制作数据并以本人身份或者以其所代表的人的名义实施电子签名的人，简称签名人。 来源：《电子签名法》
证书申请递交人	向电子认证服务机构递交证书申请的自然人,可以是订户或者订户的合法代表。 来源：GB/T 31508—2015,3.8

缩略语	**全称**
SHECA	上海市数字证书认证中心有限公司
RSP	云执钥®远程可靠电子签名服务策略
QESASC	可靠电子签名应用组件
RQESSS	远程可靠电子签名服务系统
RQESCD	远程可靠电子签名设备，由防篡改可信执行环境和符合 GM/T 0028 安全二级以上经检测认证合格的硬件密码模块组成。
DTBS	待签名数据（Data To Be Signed）
DTBSF	待签名格式化数据（Data To Be Signed Formatted）
DTBSR	待签名数据表示（Data To Be Signed Representation）
SAD	签名激活数据（Signature Activation Data）
CA	电子认证服务机构
TSA	时间戳机构
KEK	密钥加密密钥
GM/T	中国商用密码行业标准
GB/T	中国国家标准
SIC	远程可靠电子签名服务的签名交互组件

KEK	密钥加密密钥，用于加密订户私钥的对称密钥

1.6 服务使用

1.6.1 适当服务使用

根据本政策提供的服务可用于为订户提供远程电子签名服务，前提是遵守现行法律法规的规定。

1.6.2 禁止的服务使用

SHECA 远程可靠电子签名服务，禁止在如下场景中使用：

a) 涉及人身关系的，如婚姻、收养、继承等；

b) 涉及停止公共事业服务的，如停止供水、供热、供气等；

c) 法律、行政法规规定的其他不适用电子签名的应用场景或类型；

d) 国家法律法规禁止的活动。

订户不得将所获证书用于任何违法违规、违背公序良俗的用途，不得利用证书从事侵害国家利益、社会公共利益及第三方合法权益的活动。

基础级远程可靠电子签名服务不得用于涉及生命健康、财产权益等高风险应用场景。

1.7 法律与合规框架

1.7.1 适用法律法规

本服务遵循以下中国法律法规、部门规章：

a)《中华人民共和国电子签名法》（2019 年修正）

b)《中华人民共和国密码法》（2020 年施行）

c)《中华人民共和国网络安全法》（2017 年施行）

d)《中华人民共和国数据安全法》（2021 年施行）

e)《中华人民共和国个人信息保护法》（2021 年施行）

f) 《网络数据安全管理条例》（2025 年施行）

g) 《电子认证服务管理办法》（2009 年施行，2015 年修订）

h) 《电子认证服务使用密码管理办法》（2026 年修订）

1.7.2 《信息安全等级保护管理办法》合规性声明

本服务策略可能因相关法律法规的修订或监管政策的变化而进行必要调整。如有重大更新，SHECA 应至少提前 30 日通过服务网站等公开渠道通知订户及其他相关方。

1.7.3 可靠电子签名保障措施

根据《电子签名法》第十三条，可靠的电子签名须同时满足以下四项条件：

（一）电子签名制作数据用于电子签名时，属于电子签名人专有；

（二）签署时电子签名制作数据仅由电子签名人控制；

（三）签署后对电子签名的任何改动能够被发现；

（四）签署后对数据电文内容和形式的任何改动能够被发现。

依据《电子签名法》第十四条，满足上述条件的可靠电子签名与手写签名或盖章具有同等法律效力。

本服务通过以下技术安排确保满足上述可靠签名条件：

可靠电子签名条件	本服务保障措施
电子签名制作数据用于电子签名时，属于电子签名人专有	基于公钥密码算法，密钥对在符合 GM/T 0028 安全二级以上经检测认证合格的硬件密码模块中生成，可以保证电子签名制作数据（私钥）的唯一性； 公钥和电子签名认证证书与经身份标识和鉴别后的订户身份链接，可以保证属于电子签名人专有。
签署时电子签名制作数据仅由电子签名人控制	采取技术和管理手段，保证私钥激活需经过签名人身份验证与明确授权（显式确认），未经订户参与并同意，服务提供方无法使用订户私钥。

签署后对电子签名的任何改动能够被发现	使用 SM2 或 RSA 2048/ECDSA P-256 及以上强度的公钥密码算法和 SM3 或 SHA-256 及以上强度的哈希算法，数字签名具有防篡改性。
签署后对数据电文内容和形式的任何改动能够被发现	数字签名覆盖完整数据电文，篡改后可被发现。

1.7.4 法律效力声明

本服务创建的电子签名在满足上述可靠签名条件时，依照《电子签名法》具有法律效力。本服务策略不保证所有签名在任何司法管辖区都具有法律效力。 订户和依赖方有义务根据具体业务场景判断签名效力，SHECA 不承担因依赖方未能履行合理验证义务而产生的责任。

依据《电子签名法》第三条，以下情形不适用电子签名：涉及婚姻、收养、继承等人身关系的文书；涉及停止供水、供热、供气等公用事业服务的文书；法律、行政法规规定的不适用电子文书的其他情形。签名人在使用本服务时应注意避开上述禁止适用的场景。

2. 服务参与者

签名人：使用本服务创建数字签名的自然人或法人的授权使用人。

远程可靠电子签名服务提供商：运营云执钥®可靠云签名服务的实体，即 SHECA。

证书颁发机构（CA）：签发电子认证签名证书的电子认证服务机构，即 SHECA。

时间戳机构（TSA）（可选）：为签名提供时间戳的机构。

依赖方：是指基于对电子签名认证证书或者电子签名的信赖从事有关活动的实体。

其他参与方：包括调查、起诉和审判机构、监督机构以及现行法律认可的其他机构。

3. 身份鉴别与电子签名认证证书

3.1. 初始申请密钥的身份鉴别

SHECA 同步开展电子签名认证证书申请和密钥申请的身份鉴别操作，SHECA 不会将身份查验流程委托给外部机构或个人。

3.1.1. 个人身份的鉴别

有关个人身份的标识与鉴别，按照《协卡网络信任服务体系 电子签名认证证书电子认证业务规则》第 3 章规定执行。

3.1.2. 机构身份的鉴别

有关机构身份的标识与鉴别，按照《协卡网络信任服务体系 电子签名认证证书电子认证业务规则》第 3 章规定执行。

3.2. 证书续期的身份鉴别

证书续期是指在不改变证书订户主体信息的情况下，在原证书到期前，为订户签发新证书。

有关证书续期的身份标识与鉴别，按照《协卡网络信任服务体系 电子签名认证证书电子认证业务规则》4.6 规定执行。

3.3. 证书变更的身份鉴别

证书变更是指改变证书中除订户公钥之外的信息而签发新证书的情形，例如：证书订户主体名称改变等。

有关证书变更的身份标识与鉴别，按照《协卡网络信任服务体系 电子签名认证证书电子认证业务规则》4.8 规定执行。

4. 签名密钥生命周期管理

4.1. 密钥初始化

4.1.1. 密钥生成

SHECA 作为远程可靠电子签名服务系统（RQESSS）的管理者，应订户的请求并代为每个订户生成一对签名密钥对（公钥和私钥）。

密钥对生成位置：密钥对在远程可靠电子签名设备（RQESCD） 内部的硬件密码模块中生成。

证书用途：只提供签名证书，不提供加密证书。

私钥存储：除一次性签名密钥外，私钥一经生成，将以加密密文方式保存于 RQESCD 的数据库中。仅在签名人明确授权进行签名操作时，私钥可由设备内部的硬件密码模块执行签名计算，外部无法直接访问或获取私钥。

签名密钥与数字证书建立对应关系：生成的公钥通过加密通道安全发送给 CA，证书与私钥的链接关系在 RQESCD 内部受防篡改保护。

4.1.2. 身份链接

在签名密钥申请过程中，将基于订户身份鉴别结果，为私钥与订户建立唯一的链接关系。

证书签发完成后，将确立私钥与证书之间的链接关系。

订户身份鉴别环节所采集的签名人验证因素信息与签名人建立对应链接关系，这些验证因素具体包括：

a) 签名人持有的因素：例如签名人申请时预留的实名手机号、签名人设备的唯一标识等；

b) 签名人固有的因素：即签名人的生物特征，例如人脸识别信息等；

c) 签名人的知识因素：即签名人自行设定的 PIN 码。

基础级远程可靠电子签名服务，至少需要采集单因素验证信息；高等级远程可靠电子签名服务，至少需要采集双因素验证信息。

通过上述关联关系，可构建订户身份、密钥、证书、签名人验证因素之间唯一、可信且可追溯的身份链接体系。

签名人验证因素信息由签名人掌握，不可查询。

4.1.3. 一次性签名密钥

SHECA 提供一次性签名密钥，具有如下特征：

a) 密钥在身份鉴别完成后在硬件密码模块中生成，并不以任何形式导出于硬件密码模块之外；

b) 私钥对应的证书有效期为 2 小时；

c) 订户接受证书后 60 分钟内可且仅可完成单次签名（可同时包含多个待签名数据表示）；

d) 签名完成、证书过期或订户接受证书 60 分钟内未执行签名操作，私钥将立即从 RQESCD 中永久销毁；

e) 私钥不作备份、恢复和归档处理。

4.2. 私钥交付

远程可靠电子签名服务中的订户私钥不交付给订户，订户通过页面下载证书或确认同意接受即视为证书接受。

4.3. 签名激活

签名激活是指经过身份验证的签名人（或其合法授权人），使其关联特定签名私钥进入可操作状态，以执行签名运算的过程。

签名激活的基本原则：每次签名操作均须获得签名人的**显式同意**（如点击确认按钮、或提交 PIN 码等主动确认行为），不得以默认勾选或静默授权方式代替。未经签名人明示授权，SHECA 无权代表签名人调用签名私钥发起任何签名行为。

本服务依据不同安全等级，提供两种签名激活方式。

4.3.1. 基础级签名激活

签名人在本服务的客户端签名交互组件（SIC）中完成身份验证，系统将验证信息与签名人进行链接关系校验。校验通过后，即可激活对应的签名密钥，执行签名计算并返回签名值。

4.3.2. 高等级签名激活

签名人在本服务的客户端签名交互组件（SIC）中完成身份验证，并将签名人身份验证信息、待签名数据（DTBS）/待签名格式化数据（DTBSF）/待签名数据表示（DTBSR）、 签名密钥标识等相关信息进行密码学绑定，封装生成 SAD，签名人将该 SAD 提交给服务端以证明签名人已明确授权本次签名行为。

服务端（RQESCD）接收并验证 SAD 的有效性后，激活对应的签名私钥，在硬件密码模块内部完成签名运算并返回签名值。

4.3.3. 解除私钥激活状态

订户签名完成后自动解除私钥激活状态，订户如需操作私钥应再次激活。

4.4. 私钥销毁

私钥销毁触发条件，签名私钥在以下任一情况发生时须被销毁：

a) 订户主动提交密钥销毁申请并经 SHECA 批准；

b) 对应数字证书到期或被撤销后；

c) 一次性签名密钥的签名会话结束后；

d) 服务合同终止且无延续需求；

e) 若 SHECA 认为密钥有泄露的风险或证书被不适当签发，SHECA 也可以主动销毁密钥。

私钥销毁的执行方式，签名私钥销毁是在防篡改可信环境内部执行，确保：

a) 销毁后私钥数据不可恢复；

b) 内存中的私钥使用后立即不可逆转地擦除；

c) 私钥副本同步销毁；

d) 销毁过程有完整日志记录并进行审计。

订户主动申请撤销证书/销毁私钥时，SHECA 将按照与 3.1 初次申请密钥的身份鉴别要求对申请人进行身份核验。

4.5. 私钥备份与恢复

SHECA 按照最小必要范围原则，仅以灾难恢复为目的开展密钥库的备份，备份范围包括密钥、签名激活数据、及密钥与证书、订户身份、签名人验证因素的链接关系。

在容灾备份方面，SHECA 每季度至少开展一次完整的密钥库数据容灾备份。密钥备份操作必须经过业务操作员双人操作，且在全程受控的规范环境中实施；密钥备份的 KEK 实施 M 选 N 多人控制机制（M 不少于 3，N 不少于 M/2），操作应在安全认证委员会授权下进行，加密后的密钥库及相关数据以离线方式存储在 RQESCD 之外的安全介质中。

密钥恢复，必须经业务操作员多人操作方可将备份后的密钥和相关数据恢复到 RQESCD。

SHECA 不对指定的单个或多个密钥进行备份与恢复。

4.6. 会话密钥封装与恢复

云执钥®远程可靠电子签名服务不涉及会话密钥封装与恢复。

4.7. 私钥归档

不适用。

4.8. 私钥导入、导出

远程可靠电子签名服务中的订户私钥不以任何形式导出到 RQESCD 之外。

远程可靠电子签名服务中的订户私钥不接受任何形式的导入。

5. 设施、管理和操作控制

5.1. 物理安全控制

远程可靠电子签名服务部署于 SHECA 主机房的服务区，其技术设施及其控制措施，包括但不限于：场景位置与建筑、物理访问控制、电力保障、门禁与监控、灾备、环境保障措施、消防措施、设备管理、存储介质管理等按照《协卡网络信任服务体系电子签名认证证书电子认证业务规则》5.1 规定执行。

5.2. 程序控制

5.2.1. 可信角色

远程可靠电子签名服务的可信角色包括四类岗位，岗位职责如下：

a) 安全管理岗位：

1) 安全管理负责人：全面负责远程可靠电子签名服务的安全管理工作；

2) 超级管理员：添加、删除、修改业务操作员、审计管理员帐号、系统配置；

3) 业务操作员：配置系统参数；

4) 审计管理员：添加、删除、修改审计员帐号；

5) 审计员：查询操作日志、对操作记录进行抽样审计；

b) 专业技术岗位：

按照《协卡网络信任服务体系 电子签名认证证书电子认证业务规则》5.2.1 执行。

c) 对公司运营有重要影响的其他管理人员：

按照《协卡网络信任服务体系 电子签名认证证书电子认证业务规则》5.2.1 执行。

5.2.2. 需要职责分离的角色

需职责分离的角色包括：

a) 超级管理员与业务操作员；

b) 审计管理员与审计员；

c) 超级管理员与审计管理员；

d) 业务操作员与审计员；

e) 其它，按照《协卡网络信任服务体系 电子签名认证证书电子认证业务规则》5.2.2 执行。

5.3. 人员控制

按照《协卡网络信任服务体系 电子签名认证证书电子认证业务规则》5.3 规定执行。

5.4. 审计日志记录程序

记录范围：

a) 订户密钥全生命周期操作的时间、操作内容、操作结果、操作人等信息；

b) 其它，按照《协卡网络信任服务体系 电子签名认证证书电子认证业务规则》5.4.1 执行。

需要进行日志记录的关键操作与事件、记录内容，以及日志保存期限、审计内容、审计周期等，按照《协卡网络信任服务体系 电子签名认证证书电子认证业务规则》5.4 规定执行。

5.5. 记录归档

对记录（即信息和文档）归档的范围、期限与保护措施，按照《协卡网络信任服务体系 电子签名认证证书电子认证业务规则》5.5 规定执行。

5.6. 损害与灾难恢复

损害与灾难恢复的预案与流程，按照《协卡网络信任服务体系 电子签名认证证书电子认证业务规则》5.7 规定执行。

5.7. 服务可用性

SHECA 远程可靠电子签名服务的可用性不低于 99.9%。

5.8. 服务终止

SHECA 如果因技术性原因或商业原因需要终止远程可靠电子签名服务时，应遵循以下流程和通告机制，包括但不限于：

a) 起草并发布终止声明，至少提前九十日通知订户、依赖方等相关实体，并至少提前六十日向主管部门报告；

b) 自服务终止起：

1) 销毁所有订户私钥、密钥激活数据、密钥与证书/与订户身份的链接关系；

2) 及时撤销所有管理员、操作员、审计员的操作权限；

3) 对所有存档文件记录进行整理和封存；

4) 对所有敏感文档和数据进行安全处理和封存；

5) 清除主机和密码硬件设备中的敏感数据；

c) 其它，按按照《协卡网络信任服务体系 电子签名认证证书电子认证业务规则》执行。

6. 技术安全控制

6.1. 密码学、私钥及其保护

6.1.1. 密码算法

SHECA 提供下述多种算法选择，可以通过 API 指定所需算法，也可由 SHECA 根据服务等级自动选择最合适的算法：

a) 优先使用 SM2 算法（用于签名）、SM3 算法（用于哈希）；

b) 也支持使用国际通用算法（RSA 2048/3072、ECDSA P-256/P-384、SHA-256/384）。

6.1.2. 私钥生成与保护

订户密钥对在符合 GM/T 0028 安全二级及以上的、经检测认证合格的硬件密码模块内生成，并经加密后存储在防篡改可信执行环境的数据库中，KEK 应存储在符合 GM/T 0028 安全二级及以上的、经检测认证合格的硬件密码模块内。

在密钥初始化阶段（详见 4.1.2），SHECA 为每个订户建立“订户身份—签名密钥—数字证书—签名人”之间的唯一链接关系，并通过以下措施确保该链接关系在全生命周期内不可篡改、可追溯：

- **完整性校验**：采用 HMAC 对身份链接记录进行完整性保护，任何对链接关系的未授权修改均可被检测；
- **数字签名与时间戳**：链接记录的关键数据由 SHECA 的签名私钥进行数字签名并加盖可信时间戳，审计方可通过验证该签名确认记录来源的真实性与内容完整性；
- **操作审计**：所有针对链接记录的创建、修改及访问操作均须记录于受保护的审计日志中，确保全过程可审计、可追溯。

该机制为私钥的合法使用提供不可否认的身份绑定证据。

6.1.3. 私钥多人控制

本服务支持私钥的多人授权使用场。在此场景下，任何签名激活请求在进入具体验证流程前，RQESCD 将首先执行基于“合法授权使用者”关系的访问控制校验：系统验证请求中的签名人身份信息，确认其为该私钥的合法授权使用者（包括订户本人、以及经订户合法授权的其他自然人）。只有当身份验证通过、授权关系处于有效期内、且目标私钥确实授予该签名人使用权限时，激活流程方可继续。任何不在授权列表中的签名人请求激活该私钥，将被系统无条件拒绝。

6.1.4. 私钥销毁

见本文件 4.4 规定。

6.1.5. 私钥备份与恢复

见本文件 4.5 规定。

6.1.6. 远程电子签名安全保障

无论基础级还是高等级签名服务，签名私钥均由符合 GM/T 0028 安全二级及以上的硬件密码模块生成，以加密形式存储于防篡改可信执行环境（RQESCD）中，私钥的明文形式绝不离开硬件密码模块的物理边界，外部系统（包括 SHECA 运维人员、上层业务系统、签名交互组件）无法读取、导出或复制私钥明文。所有签名运算均在硬件内部完成，签名完成后私钥立即退出激活状态。

在此基础上，远程可靠电子签名全流程各环节提供如下保护措施：

身份认证：签名人须通过身份验证后方可激活私钥。系统校验签名人身份与私钥的身份链接关系，确认当前操作者为订户本人或其合法授权人。基础级采用单因素认证，高等级采用双因素/多因素强认证（详见下文高等级特别说明）。

待签名数据呈现：在签名运算前，SIC 将待签名数据（或其 DTBSF/DTBSR）呈现给签名人确认；系统确保 RQESCD 不更改 DTBS（或其 DTBSF/DTBSR），且被签名的数据与签名人确认的数据一致（详见 4.3.4）。

签名授权凭证构造与传输：认证凭证及签名指令（含 SAD、DTBS/DTBSF/DTBSR）通过加密安全信道传输，防止在传递过程中被窃听、篡改或重放。

私钥激活：系统验证签名人身份和授权关系有效后，在硬件内部将对应的签名私钥从“休眠”状态临时置于“可操作”状态，随即执行签名运算。签名完成后私钥自动退出激活状态。基础级校验签名人身份链接关系，高等级额外校验 SAD 完整性与真实性。

签名运算：签名运算在硬件密码模块内部执行，使用标准非对称密码算法对待签名数据摘要进行计算，签名结果具有密码学意义上的不可伪造性。

审计追溯：每次私钥调用均生成不可篡改的操作记录，包含调用时间、签名人身份、操作结果等信息，并按本文件 5.4 和 5.5 的规定完成存储、审计和归档。SHECA 向订户提供私钥调用记录查询服务，查询前按照 3.1 的要求对订户进行身份鉴别。

6.2. 计算机安全控制

按照《协卡网络信任服务体系 电子签名认证证书电子认证业务规则》6.6 规定执行。

6.3. 生命周期安全控制

按照《协卡网络信任服务体系 电子签名认证证书电子认证业务规则》6.7 规定执行。

6.4. 网络安全控制

按照《协卡网络信任服务体系 电子签名认证证书电子认证业务规则》6.8 规定执行。

7. 合规审计和其他评估

7.1. 评估频率或情形

SHECA 作为运营主体，至少每年进行一次内部一致性审计和评估，以保证远程可靠电子签名服务的可靠性、安全性和可控性。

若法律法规和监管部门要求，SHECA 还应进行外部审计和评估。

7.2. 评估者的身份/资格

在进行内部评估审计时，SHECA 要求评估人员至少具备电子认证、密码技术、信息安全审计的相关知识，有二年以上的相关经验，以及应具备计算机、网络、信息安全等方面的知识和实际工作经验。内部评估由战略发展部组织实施。

SHECA 依据法律法规和监管要求，选取符合标准的外部审计评估机构。

7.3. 评估者与被评估者的关系

内部评估人员需保持岗位独立性，与被评估业务或部门无利益关联。

外部评估者和 SHECA 之间是独立的关系，没有任何利害关系足以影响评估的客观性，评估者应以独立、公正、客观的态度对 SHECA 进行评估。

7.4. 评估内容

SHECA 和外部审计评估机构依据法律法规、标准规范、监管要求和本服务策略开展审计评估工作。

7.5. 对问题与不足采取的措施

审计评估完成后，SHECA 必须根据评估的结果检查缺失和不足，根据评估者提出的整改要求，提交修改和预防措施以及整改计划书，并接受其对整改计划的审查，以及对整改情况的再次评估。

7.6. 评估结果的传达与发布

内部审计评估结果以书面报告形式提交给 SHECA 安全认证委员会和公司管理层。

外部审计评估结果的发布，按政策法规和监管要求执行。

8. 法律责任和其他业务条款

8.1. 费用

按照《协卡网络信任服务体系 电子签名认证证书电子认证业务规则》9.1 规定执行。

8.2. 财务责任

按照《协卡网络信任服务体系 电子签名认证证书电子认证业务规则》9.2 规定执行。

8.3. 业务信息的保密

按照《协卡网络信任服务体系 电子签名认证证书电子认证业务规则》9.3 规定执行。

8.4. 个人信息的隐私

按照《协卡网络信任服务体系 电子签名认证证书电子认证业务规则》9.4 规定执行。

8.5. 知识产权

按照《协卡网络信任服务体系 电子签名认证证书电子认证业务规则》9.5 规定执行。

8.6. 声明与保证

8.6.1. 服务机构的声明与保证

SHECA 保证：

a) 通过 www.sheca.com 上提供的联系方式进行服务运营的技术支持、处理非标准情况以及服务运营咨询；

b) 服务始终在法律和技术上保持最新，并符合相关法律和技术标准与规范。

所有保证及由此产生的履行仅在客户未违反合同义务的情况下可被认可。

8.6.2. 其他参与方的声明与保证

不适用于本文件。

8.7. 担保免责

按照《协卡网络信任服务体系 电子签名认证证书电子认证业务规则》9.7 规定执行。

8.8. 责任限制

按照《协卡网络信任服务体系 电子签名认证证书电子认证业务规则》9.8 规定执行。

8.9. 赔偿

按照《协卡网络信任服务体系 电子签名认证证书电子认证业务规则》9.9 规定执行。

8.10. 有效期与终止

按照《协卡网络信任服务体系 电子签名认证证书电子认证业务规则》9.10 规定执行。

8.11. 对参与者的个别通告与沟通

按照《协卡网络信任服务体系 电子签名认证证书电子认证业务规则》9.11 规定执行。

8.12. 修订和发布

见本文件 1.3。

8.13. 争议处理与举证

按照《协卡网络信任服务体系 电子签名认证证书电子认证业务规则》9.13 规定执行。

8.14. 管辖法律

按照《协卡网络信任服务体系 电子签名认证证书电子认证业务规则》9.14 规定执行。

8.15. 与适用法律的符合性

按照《协卡网络信任服务体系 电子签名认证证书电子认证业务规则》9.15 规定执行。

8.16. 一般条款

按照《协卡网络信任服务体系 电子签名认证证书电子认证业务规则》9.16 规定执行。

8.17. 其他条款

按照《协卡网络信任服务体系 电子签名认证证书电子认证业务规则》9.17 规定执行。