北京群盾科技有限公司
电子认证业务规则

(版本号:V1.1.2)

修订日期：2023.2.6

审批日期：2023.2.6

发布日期：2023.2.6

目 录

文件版本说明

版本	发布时间	修订说明	审核
1.0.1	2022.8.16	初稿	公司安全策略管理委员会
1.1.1	2023.1.9	修订审计间隔、身份鉴别方式	公司安全策略管理委员会
1.1.2	2023.2.6	修订1.5.4、5.4.2及个别地方用词	公司安全策略管理委员会

1. 概括性描述

1.1. 概述

北京群盾科技有限公司电子认证业务规则（以下简称《群盾CA电子认证业务规则》，《电子认证业务规则》或《群盾CA CPS》）由北京群盾科技有限公司按照国家工业和信息化部《电子认证服务管理办法》的要求，依据《电子认证业务规则规范(试行)》制定，并报国家工业和信息化部备案。

北京群盾科技有限公司(简称“群盾CA”）于2022年8月开始运营。群盾CA严格按照《中华人民共和国电子签名法》和《电子认证服务管理办法》的要求，以及相关管理规定，提供数字证书受理、颁发、存档、更新、查询、废止等服务，并通过以密码技术、数字证书应用技术为核心的应用安全解决方案，为电子商务、电子政务和企业信息化构建安全、可靠的信任环境。

本文详细阐述了群盾CA在实际工作和运行中所遵循的各项规范。本《电子认证业务规则》适用于群盾CA、注册机构、订户和依赖方，各参与方必须完整地理解和执行本《电子认证业务规则》所规定的条款，并承担相应的责任和义务。

1.2. 文档名称与标识

文档名称是《北京群盾科技有限公司电子认证业务规则》V1.1.2，在本文件中其他地方将以《群盾CA电子认证业务规则》、《电子认证业务规则》或《群盾CA CPS》指代本文件。

1.3. 电子认证活动参与方及其职责

1.3.1 电子认证服务机构

群盾CA是根据《中华人民共和国电子签名法》、《电子认证服务管理办法》规定依法设立的第三方电子认证服务机构。群盾CA通过给从事电子交易活动的各方主体颁发数字证书、提供证书验证服务等手段而成为电子认证活动的参与主体。

1.3.2 注册机构

注册机构作为电子认证服务机构授权的下属机构，负责证书订户信息的审核、整理汇总、统计分析，与上级CA进行数据交换，管理和服务下层注册分支机构和下层受理点。每个注册机构可以按照行业或行政地域分成多个注册分支机构，或直接连接受理点，可以直接对最终订户提供服务。注册机构有责任妥善保存订户的数据，不允许将订户的数据透露给与证书申请无关的任何单位或个人，不允许用作商业利益方面的用途。

注册机构可以由群盾CA自建或授权的第三方机构建立。当注册机构由第三方机构建立时，群盾CA必须与其签订协议，明确双方的权利和义务。

1.3.3 订户

指接受并持有群盾CA颁发的证书终端实体，包括个人、企业和组织机构。

1.3.4 依赖方

依赖方是依赖于证书真实性的实体。在电子签名应用中，即为电子签名依赖方。依赖方可以是、也可以不是一个订户。在群盾CA证书服务体系中，是信任群盾CA证书，可以对使用群盾CA证书机制进行的数字签名进行验证，使用其他群盾CA证书的公钥加密信息的实体。

1.3.5 其他参与者

其他参与者指为群盾CA服务体系提供相关服务的其他实体。比如在证书申请审批过程中，提供实体身份确认服务的权威第三方。除了电子认证服务机构、注册机构、订户以及依赖方以外的参与方统一称为其他参与者。

1.4. 证书应用

群盾CA签发的数字证书可以在电子商务、电子政务等领域应用。证书应用场景下，各业务系统开发商均需满足国家相关法律法规及技术标准要求。

1.4.1 适合的证书应用

数字证书可确保互联网上信息传递双方身份的真实性、信息的保密

性和完整性、以及网上交易的不可否认性。

群盾CA数字证书可以在电子政务社会管理和公共服务、电子交易、电子办公、电子公证、公共服务等领域应用，为建设互联网络的信任环境开展了基础性的服务。根据证书的功能以及使用证书的实际应用，目前群盾CA签发的主要证书类型包括：

1) 个人证书：个人包括自然人或特定身份的人员，如公务员、企业员工等。此类证书通常用于数字签名、加密解密、安全电子邮件以及网上身份认证等，在不违背相关法律法规、群盾CA CPS以及订户协议的情况下，此类证书也可以用于其他用途；

2) 机构证书：机构包括企事业单位、政府机关、社会团体等。此类证书通常用于数字签名、加密解密以及网上身份认证等，在不违背相关法律法规、群盾CA CPS以及订户协议的情况下，此类证书也可以用于其他用途；

3) 设备证书：设备包括服务器、防火墙、路由器等，此类证书通常用于网上设备的身份认证，在不违背相关法律法规、群盾CA CPS以及订户协议的情况下，此类证书也可以用于其他用途。

1.4.2 限制的证书应用

群盾CA发放的数字证书、提供的各类安全接口禁止在违反国家法律、法规或破坏国家安全的情况下使用，由此造成的法律后果由订户承担。

证书使用前，依赖方有义务调用群盾CA所提供的证书验证接口、黑名单或实时在线查询协议查询证书的有效性。如因依赖方不对有效性进

行查询而导致证书被误用，由此造成的法律后果由依赖方承担。

1.5. 策略管理

1.5.1 策略文档管理机构

管理本文档的机构是：群盾CA安全策略管理委员会。

1.5.2 联系信息

群盾CA将对电子认证业务规则进行严格的版本控制，并由群盾CA指定专人负责。

联系地址：北京市海淀区北清路中关村壹号天地融大厦

邮编：100094

电话：+(86)010-82068888

电子邮件：support@tendyron.com

网址：http://www.trondun.com

1.5.3 决定CPS符合策略的机构

决定CPS符合策略的机构为：群盾CA安全策略管理委员会。

1.5.4 CPS批准流程

按照信息产业部公布的《电子认证业务规则规范》的要求，在群盾CA电子认证业务做出任何变动之前，群盾CA安全策略管理委员会将对提供的变动建议进行研究，在征询群盾CA法律顾问有关方面的意见后，提

交群盾CA安全策略管理委员会审批。群盾CA根据《电子认证服务管理办法》中规定，在本机构网站（http://www.trondun.com）予以公布，并自公布之日起三十日内向工业和信息化部备案。

1.6. 定义和缩写

1）群盾CA

群盾CA是北京群盾科技有限公司的简称，是根据《中华人民共和国电子签名法》、《电子认证服务管理办法》规定依法设立的第三方电子认证服务机构。群盾CA的关联单位包含群盾CA授权的注册机构、注册分支机构、受理点等证书体系成员。

2）《群盾CA CPS》

《群盾CA CPS》全称是《北京群盾科技有限公司电子认证业务规则》，在本文件中其他地方将以《群盾CA电子认证业务规则》、《电子认证业务规则》指代本文件。

3）公开密钥基础设施（PKI）

公开密钥基础设施（Public Key Infrastructure，简称PKI）是利用公钥加密技术为电子认证的开展提供一套安全基础平台的技术和规范。它能够为所有网络应用提供加密和数字签名等密码服务及所必需的密钥和证书管理体系，提供互联网环境的身份鉴别、信息加解密、数据完整性和不可否认性服务。

4）电子认证服务机构（CA）

电子认证服务机构（Certification Authority，简称CA）是受订户

信任的，负责签发数字证书的权威机构，又称为数字证书认证中心。作为电子交易中受信任的第三方，负责为电子认证业务中各个实体颁发数字证书，以证明各实体身份的真实性，并负责在交易中检验和管理证书。

5) 注册机构（RA）

注册机构（Registration Authority，简称RA）是负责订户证书的申请、审批和证书管理部分工作，面向证书订户。

6) 数字证书（Digital Certificate）

数字证书是指经CA数字签名的包含数字证书使用者身份公开信息和公开密钥的电子文件。数字证书提供了一种在Internet上验证身份的方式，其作用类似于日常生活中的身份证。

7) 证书撤销列表（CRL）

证书撤销列表(Certificate Revocation List，简称CRL)，是一种包含撤销的证书列表的签名数据结构。CRL是证书撤销状态的公布形式，就像信用卡的黑名单，它通知其他证书订户某些电子证书不再有效。

8) 在线证书状态协议（OCSP）

在线证书状态协议是用于检查数字证书在某一交易时间是否有效的标准。

9) 证书策略（CP，Certificate Policy）

证书策略（Certificate Policy，简称 CP）是一套命名的规则集，用以指明证书对一个特定团体和（或者）具有相同安全需求的应用类型的适用性。

10) 电子认证业务规则（Certificate practice Statement ，简称

CPS）

电子认证业务规则（Certificate Practice Statement，简称 CPS）是关于CA的颁发和管理证书的运做规范的描述，包括CA整体运行规范和证书的颁发、管理、撤销和密钥以及证书更新的操作规范等事务。

11) 私钥（Private key）

私钥（Private key）是在公钥基础设施 PKI 中为一个密码串，由特定算法与公钥一起生成，用于解密信息或进行数字签名。在数字签名中又称为电子签名制作数据，是在电子签名过程中使用的，将电子签名与电子签名人可靠地联系起来的字符、编码等数据。

12) 公钥(Public key)

公钥(Public key)是在公钥基础设施（PKI）中为一个密码串，由特定算法与私钥一起生成，用于加密信息或验证数字签名。在数字签名中又称为电子签名验证数据，是用于验证电子签名的数据，包括代码、口令等。

13) 甄别名(DN , Distinguished Name)

甄别名(DN , Distinguished Name)是在数字证书的主体名称域中，用来唯一标识订户的 X.500 名称。此域需要填写反映订户真实身份的、具有实际意义的、与法律不冲突的内容。

14) X.509

X.509 是 ITU 制定的 X.500 系列的目录标准的其中一个。它为公钥证书定义了一个框架。

15) KMC(Key Management Center)

KMC(Key Management Center)密钥管理中心的简称。用于产生订户加密证书密钥对，并提供加密密钥对托管服务的管理机构。

2. 信息发布与信息管理

2.1. 认证信息的发布

群盾 CA 电子认证系统信息库包括以下内容：CPS、证书、CRL。群盾CA的职责是确保发布的认证信息及时、可靠。

根据我国法律法规的要求以及 X.509 标准，群盾CA在对外的目录服务器（Directory Server）公布证书相关信息，并以定期和实时的方式公布证书撤销列表CRL。

2.2. 公众信息的发布

2.2.1 CPS的发布

群盾CA通过公司网站（http://www.trondun.com）发布本机构制定的CPS，并负责本规范的解释，一经群盾CA在网站或以书面声明形式发布、更改，即时生效，并对一切仍有效的数字证书使用者、新的数字证书及相关业务的订户均具备约束力。

本规则的发布及更改一律须经群盾CA核准和发布。如有需要可访问群盾CA网站查看本电子认证业务规则，对具体个人不另行通知。

2.2.2 群盾CA公众信息的发布

群盾CA在公司网站http://www.trondun.com上发布与其相关的公众信息，并对旧信息进行处理。已有旧信息与群盾CA新发布的信息不一致的，以群盾CA新发布的信息为准。

2.3. 发布时间或频率

《群盾CA电子认证业务规则》一经网站发布，即时生效。对数字证书的订户及证书申请人均具备约束力。对具体个人不另行通知。

群盾CA的证书废除列表（CRL）每24小时发布一次，在24：00点整更新。

2.4. 信息库访问控制

对于公开发布的CPS、CRL等公开信息，群盾CA允许公众自行通过网站和合法途径进行查询和访问。

只有经授权的RA/CA管理员可以查询群盾CA和注册机构数据库中的其他数据。

3. 身份标识与鉴别

3.1. 命名

3.1.1 名称类型

每个订户对应一个甄别名（DistinguishedName，简称DN）。

数字证书中的主体的X.509 DN是C=CN命名空间下的X.509目录唯一名字。其通用名包含于每张证书的主题中，唯一标识证书订户的身份。各类证书命名方式不同，但是所有证书订户名都需要严格审查，命名符合X.500甄别名规定。

3.1.2 对名称意义化的要求

订户的甄别名(DN)必须具有一定的代表意义。

证书主体名称标识本证书所提到的最终实体的特定名称，描述了与主体公钥中的公钥绑定的实体信息。

3.1.3 订户的匿名或伪名

在群盾CA证书服务体系中，不接受匿名或伪名，必须使用有明确意义的名称作为唯一标识符。

3.1.4 理解不同名称形式的规则

DN的具体内容依次由CN、OU、O、C四部分组成。其中CN用来表示实体名，OU、O用来表示组织单位名称、C用来表示国家。特殊情况下，命

名规则根据项目情况而定，但不超出X.509相关标准之命名方式。

3.1.5 名称的唯一性

在群盾CA证书服务体系中，群盾CA保证签发给某个实体的证书，其主题甄别名（含群盾CA对证书赋予的唯一识别号）在CA信任域内是唯一的。

3.1.6 商标的承认、鉴别和角色

群盾CA签发的证书的主题甄别名中将不包含商标名，不存在此类业务场景。

3.2. 初始身份确认

3.2.1 证明持有私钥的方法

群盾CA证明拥有私钥的方法是根据证书申请信息进行验证。首先利用数据摘要算法进行计算，再用申请信息中的公钥对申请信息中的签名解密，然后进行比较，如果相等则证明数字证书的订户拥有与签名验证公钥对应的签名私钥。

3.2.2 组织身份的鉴别

对于组织机构订户，群盾CA或注册机构需鉴别：订户提交的组织身份信息、组织授予经办人的授权证明、经办人的个人身份证明材料。

对于订户提交的组织身份信息，鉴别方式包括核对订户提交的组织有效身份证件或证件的具体信息，必要时可以通过权威第三方数据库信

息比对。组织有效身份证件是指政府部门签发的证件或文件，包括但不限于营业执照、事业单位登记证、社会团体登记证、政府批文等。

对于组织授予经办人的授权证明，鉴别方式包括但不限于检查组织或组织的法定代表人授权给经办的办理证书事宜的授权文件。

鉴别方式可以采用面对面现场鉴别。当群盾CA或注册机构认为有需要时，可以增加其他方式，包括但不限于鉴别组织的法定代表人身份或要求经办人提交法定代表人有效身份证件证明。

鉴别审核批准申请后，群盾CA或注册机构按照相关法律的要求妥善保存订户申请材料，群盾CA保存订户申请材料可以是纸质或电子数据形式。

群盾CA身份鉴证规则简要说明了如何进行个人身份鉴别。群盾CA保留根据最新国家政策法规的要求更新组织身份鉴别方法与流程的权利。

3.2.3 个人身份的鉴别

对于个人订户，群盾CA或注册机构将验证个人有效身份证件或证件的具体信息，核实个人订户身份的真实性。个人有效身份证件指政府部门签发的证件，包括但不限于：身份证、港澳台居民身份证、户口簿、护照、军官证等。

鉴别方式可以采用面对面现场鉴别。必要时，可以通过权威第三方数据库信息比对、手机短信验证等其他可靠的方式鉴别。

鉴别审核批准申请后，群盾CA或注册机构按照相关法律的要求妥善保存订户申请材料，群盾CA保存订户申请材料可以是纸质或电子数据形

式。

群盾CA身份鉴证规则简要说明了如何进行个人身份鉴别。群盾CA保留根据最新国家政策法规的要求更新个人身份鉴别方法与流程的权利。

3.2.4 设备身份的鉴别

申请人申请设备证书，除依据申请人身份的不同类别，按本文§3.2.2组织身份的鉴别和§3.2.3个人身份的鉴别证明申请人的身份外，还须证明对相应设备的识别信息拥有权。所称的设备包括设备名称、域名地址、IP 地址、账号等。

群盾CA 或其 RA 的业务受理人员在认为有必要的情况下，采取第三方信息数据或服务鉴定订户身份及申请人对设备的拥有权，申请人有配合业务受理员的调查工作的义务。

3.2.5 没有验证的订户信息

未在前面所列的，对于不影响订户身份追溯的信息，群盾CA一般不予验证。

3.2.6 授权确认

为确保办理人具有特定的许可，代表组织获取数字证书，需要出具组织授权其该组织为办理群盾CA数字证书事宜的授权文件。

组织在群盾CA的数字证书申请表上加盖单位公章后，则证明本组织对办理人的授权确认。

3.2.7 互操作准则

对于群盾CA外的其他证书服务机构颁发的证书，可以与群盾CA进行互操作，但是必须符合群盾CA的证书策略的要求，并且与群盾CA签署了相应的协议。

3.3. 密钥更新请求的身份标识与鉴别

3.3.1 常规密钥更新的标识与鉴别

对于常规密钥更新，订户可以用原有的私钥对更新请求进行签名。群盾CA认证系统会对订户的签名和更新请求进行鉴别。

订户也可以选择一般的初始证书申请流程，按照初始身份验证步骤（详细内容请见§3.2）进行常规密钥更新，按照要求提交相应的证书申请和身份证明资料。

群盾CA授权的注册机构的审核人员合理、审慎地核对申请材料，根据审核人员的管理规定对订户的资料的真实性进行审查，并进行批准或拒绝的操作。

密钥更新会造成使用原密钥对加密的文件或数据无法解密，因此，订户在申请密钥更新前，必须确认使用原密钥对加密的文件或数据已经解密，由此造成的损失，群盾CA将不承担责任。

3.3.2 撤销后密钥更新的标识与鉴别

撤销后证书不进行密钥更新。等同于订户重新申请证书，身份标识和鉴别的要求，使用原始身份验证相同的流程，详见§3.2.2组织身份的

鉴别和§3.2.3个人身份的鉴别。

3.4. 撤销请求的标识与鉴别

在群盾CA的证书业务中，证书撤销请求可以来自订户，也可以来自群盾CA或注册机构。

订户本人撤销时的身份标识和鉴别使用原始身份验证相同流程，详见§3.2.2组织身份的鉴别和§3.2.3个人身份的鉴别。

如果是因为订户没有履行本《电子认证业务规则》所规定的义务，有注册机构申请撤销订户的证书时，不需要对订户身份进行标识和识别。

4. 证书生命周期操作要求

4.1. 证书申请

4.1.1 证书申请实体

证书申请实体包含个人、企业单位、事业单位、社会团体、人民团体等各类组织机构以及CA、RA、受理点和CA机构或RA机构的系统及相应的管理员。

4.1.2 申请过程与责任

群盾CA目前只接受面对面申请方式，申请程序根据群盾CA证书的种类不同而不同，但都应遵守证书操作所规定的步骤。设备证书包含服务器证书、软件代码、支付网关证书以及其他证书。

证书申请流程如下：

1) 对于个人证书（包括个人身份证书，个人安全电子邮件证书，个人代码签名证书），订户到群盾CA授权的注册机构领取证书申请表（一式一份）或到群盾CA网站下载相应的申请表（一式一份），并提供个人身份证明文件及其复印件一份，例如：身份证、军官证、学生证、护照等。详细内容请见§3.2。

2) 对于单位证书（包括单位身份证书，单位安全电子邮件证书，单位代码签名证书），订户到群盾CA授权的注册机构领取单位证书申请表（一式一份）或到群盾CA网站下载相应的申请表（一式一份），订户应提供单位对经办人的授权委托书，单位的营业执照、税务登记证、组织机构代码证、经办人的身份证和群盾CA可能需要的其他文件。详细内容请见§3.2。

3) 对于设备证书，与单位的申请相同，还需要提供服务器域名的所有权的证明，详细内容请见§3.2。

4) 对于其他类型证书，群盾CA网站上发布申请要求，并且群盾CA拥有解释权。

5) 对于群盾CA测试证书、内部通讯证书、管理员证书、操作员证书或注册机构、注册分支机构的通讯证书、管理员证书，要填写群盾CA内部证书申请表；对于注册机构、注册分支机构下的所有证书申请表，需一式一份。

订户的申请表和相关证明文件的复印件存档 5 年。

群盾CA作为电子认证服务的发证机构有责任对申请人的身份进行充

分的验证。出于安全性和审查的需要，申请表应由验证人签名并注明日期。详细内容请见§3.2。

订户必须真实填写证书申请信息，并遵守《电子认证业务规则》。否则，群盾CA有权拒绝签发证书、停止证书的使用、废止证书，且由此造成的后果，群盾CA不承担任何责任。

4.2. 证书申请处理

4.2.1 执行识别与鉴别功能

群盾CA或授权的注册机构按照《群盾CA电子认证业务规则》所规定的身份鉴别流程对申请人的身份进行识别与鉴别。具体的鉴别流程详见§3.2.2组织身份的鉴别、§3.2.3个人身份的鉴别和§3.2.4设备身份的鉴别。

4.2.2 证书申请批准和拒绝

群盾CA或授权的注册机构根据《群盾CA电子认证业务规则》所规定的身份鉴别流程对证书申请人身份进行识别与鉴别后，根据鉴别结果决定批准或拒绝证书申请。

如果证书申请人通过《群盾CA电子认证业务规则》所规定的身份鉴别流程且鉴证结果为合格，群盾CA或注册机构将批准证书申请，为证书申请人制作并颁发数字证书。

证书申请人未能通过身份鉴证，群盾CA或注册机构将拒绝申请人的证书申请，并通知申请人鉴证失败，同时向申请人提供失败的原因(法律

禁止的除外)。

被拒绝的证书申请人可以在准备正确的材料后，再次提出申请。

4.2.3 处理证书申请的时间

群盾CA授权的注册机构将做出合理努力来尽快确认证书申请信息，一旦注册机构收到了所有必须的相关信息，将在2个工作日内处理证书申请。

注册机构能否在上述时间期限内处理证书申请取决于证书申请人是否真实、完整、准确地提交了相关信息和是否及时地响应了群盾CA的管理要求。

4.3. 证书签发

4.3.1 证书签发过程中电子认证服务机构的行为

订户一旦提交了证书申请，尽管事实上还没有接受证书，但该订户仍被视为已同意发证机构签发其证书。

群盾CA授权的注册机构批准证书申请后（参见§4.2），接收参考码、授权码，为证书订户制作证书，并提供给订户。

证书的发行意味着群盾CA最终完全正式地批准了证书申请。证书从订户接受证书（参见§4.4）之日起将被视为有效证书。

4.3.2 电子认证服务机构对订户的通告

对于订户的证书申请，无论是拒绝或批准，注册机构通过两种方式

提供证书，现场实时申领与特定场景通告，特定场景通告对订户的通告有以下几种方式：

1)通过面对面的方式，通知订户到注册机构领取数字证书；注册机构把证书等直接提交给订户，来通知订户证书信息已经正确生成；

2)其他群盾CA认为安全可行的方式通知订户。

4.4. 证书接受

4.4.1 构成接受证书的行为

在群盾CA数字证书签发完成后，群盾CA将把数字证书当面或其他群盾CA认为安全可行的方式交给订户，订户从获得证书起就被视为已同意接受证书。订户接受数字证书后，应妥善保存其证书对应的私钥。

4.4.2 电子认证服务机构对证书的发布

群盾CA在签发完证书后，就将证书发布到数据库和对外目录服务器上。

群盾CA采用主、从目录服务器结构来发布所签证书。签发完成的数据直接写入主目录服务器中，然后通过主从映射，将主目录服务器的数据自动同步到从目录服务器中，供订户和依赖方查询和下载。

4.4.3 电子认证服务机构在颁发证书时对其他实体的通告

对于群盾CA签发的证书，群盾CA不对其他实体进行通告，订户和依赖方可以在目录服务器上自行查询。

4.5. 密钥对和证书的使用

群盾CA要求订户密钥对和证书的使用不能超过其规定使用范围，否则群盾CA不承担由订户违规使用而造成的任何责任。

4.5.1 订户私钥和证书的使用

订户在提交了证书申请并接受了群盾CA所签发的证书后，均视为已经同意遵守与群盾CA、依赖方有关的权利和义务的条款。订户接受到数字证书，应妥善保存其证书对应的私钥。

订户只能在指定的应用范围内使用私钥和证书，订户只有在接受了相关证书之后才能使用对应的私钥，并且在证书到期或被撤销之后，订户必须停止使用该证书对应的私钥。

4.5.2 依赖方对公钥和证书的使用

依赖方只能在恰当的应用范围内依赖于证书，并且与证书要求相一致（如密钥用途扩展等）。依赖方获得订户的证书后，可以通过查看证书了解订户的身份，并通过证书公钥验证订户电子签名的真实性。

验证证书的有效性包括三个方面的内容：

1)用群盾CA的证书验证证书中的签名，确认该证书是群盾CA签发的，并且证书的内容没有被篡改。

2)检验证书的有效期，确认该证书在有效期之内。

3)查询证书状态，确认该证书没有被注销。

在验证电子签名时，依赖方应准确知道什么数据已被签名。在公钥

密码标准里，标准的签名信息格式被用来准确表示签名过的数据。

4.6. 证书更新

4.6.1 证书更新的情形

在证书上都有明确的证书有效期，表明该证书的起始日期与截至日期。订户应当在证书有效期到期前，到群盾CA授权的注册机构申请更新证书。

4.6.2 请求证书更新的实体

订户可以请求证书更新。

4.6.3 证书更新请求的处理

订户或其授权人通过已有私钥，在群盾CA授权的注册机构通过PIN码验证和身份信息核查，进行更新请求；或在群盾CA授权的注册机构书面填写《群盾CA数字证书申请表》。群盾CA授权的注册机构按照§4识别与鉴定的规定对订户提交的证书更新申请进行审核。发证机构审核通过后，为订户制作证书；证书签发后，发证机构将证书当面发给订户。订户接受证书（参见§4.4）；新证书签发后原有证书将被撤销（参见§4.9）。群盾CA将实时在LDAP上发布订户的新证书。订户被撤销的原有证书将在24小时内通过CRL发布。

提出更新申请的订户在进行证书更新之前应将加密邮件等加密过的文件进行解密，同时备份（例如将邮件内容复制以明文方式存储或将邮

件附件保存），然后将证书删除。以上操作完成后才能进行证书的更新。如订户未解密文件而进行证书更新，由此造成的可能损失，群盾CA不承担任何责任。

4.6.4 颁发新证书时对订户的通告

同§4.3.2。

4.6.5 构成接受更新证书的行为

同§4.4.1。

4.6.6 电子认证服务机构对更新证书的发布

同§4.4.2。

4.6.7 电子认证服务机构在颁发证书时对其他实体的通告

同§4.4.3。

4.7. 证书密钥更新

4.7.1 证书密钥更新的情形

密钥更新请求的处理方式是换发新证书。

1）证书的有效期将要到期，证书更新。

2）怀疑私钥泄漏，可以通过证书更新方式申请新证书而撤销旧证书。

3）其他。

4.7.2 请求证书密钥更新的实体

请求证书密钥更新的实体同§4.6.2。

4.7.3 证书密钥更新请求的处理

密钥更新请求的处理方式是换发新证书。

4.7.4 颁发新证书对订户的通告

颁发新证书给订户的通告同§4.3.2。

4.7.5 构成接受密钥更新证书的行为

正式接受密钥更新证书的行为同§4.4.1。

4.7.6 电子认证服务机构对密钥更新证书的发布

群盾CA对密钥更新证书的发布同§4.4.2。

4.7.7 电子认证服务机构在颁发证书时对其他实体的通告

群盾CA在颁发证书时对其他实体的通告同§4.4.3。

4.8. 证书变更

4.8.1 证书变更的情形

证书变更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。订户证书只有在有效期内，才可能发生证书变更的情况。

证书变更的原因有：

1）证书订户甄别名更改；

2）其他：如通用名、组织、角色改变等原因。

4.8.2 请求证书变更的实体

订户可以请求证书变更。

4.8.3 证书变更请求的处理

对于要求证书变更的，需确认证书变更请求是被订户或订户授权的代表提出的，并对其身份进行鉴别。证书处理过程同§4.6.3“证书更新请求的处理”。证书变更后，证书的有效期并没有改变，仍然为原证书有效期。

4.8.4 颁发新证书时对订户的通告

同§4.7.4。

4.8.5 构成接受变更证书的行为

同§4.4.1。

4.8.6 电子认证服务机构对变更证书的发布

同§4.4.2。

4.8.7 电子认证服务机构对其他实体的通告

同§4.4.3。

4.9. 证书撤销和挂起

4.9.1 证书撤销的情形

证书撤销是指由于各种原因导致证书不能再继续使用，必须废除的情况。证书撤销的原因主要有：

1) 新的密钥对替代旧的密钥对；

2) 密钥失密：与证书中的公钥相对应的私钥被泄密或订户怀疑自己的密钥失密；

3) 从属关系改变：与密钥相关的订户的主题信息改变，证书中的相关信息有所变更；

4) 操作中止：由于证书不再需要用于原来的用途，但密钥并未失密，而要求中止（例如订户离开了某个组织）；

5) 证书到期：到期后订户未续约；

6) 订户不能履行电子认证业务规则或其他协议、法律及法规所规定的责任和义务；

7) 订户申请初始注册时，提供不真实材料；

8) 证书已被盗用、未经授权的泄漏和其它安全威胁；

9) CA失密：电子认证服务机构因运营问题，导致CA内部重要数据或CA根密钥失密等原因；

10) 订户自动提出撤销请求；

11) 其他情况。这些情况可以是因法律或政策的要求群盾CA采取的临时撤销措施，也可以是订户申请撤销证书时填写的其他原因。

4.9.2 请求证书撤销的实体

请求证书撤销的实体包括：

1）订户本人或其授权代表；

2）群盾CA或其授权机构的授权代表；

3）司法机关等公共权力部门的授权代表。

4.9.3 撤销请求的流程

订户到群盾CA授权的注册机构书面填写《群盾CA数字证书申请表》，并注明撤销的原因。群盾CA授权的注册机构按照§3识别与鉴定的规定对订户提交的证书撤销申请进行审核。群盾CA撤销订户证书后，发证机构将当面通知订户证书被撤销。

如是强制撤销，群盾CA授权的发证机关管理员可以对订户证书进行强制撤销，撤销后必须立即通知该证书订户。强制撤销的命令来自于群盾CA、群盾CA授权的注册机构或司法机关等公共权力部门。

订户证书在24小时内进入CRL或被直接签发CRL，向外界公布。

4.9.4 撤销请求宽限期

当最终订户发现出现第 4.9.1 章节中的情况时，应该尽快提出证书撤销请求，撤销请求必须在密钥泄密或有泄密嫌疑8小时以内发现提出，其它撤销原因从发现需要撤销证书到向群盾CA或注册机构提出撤销请求的时间间隔必须在24小时以内提出。

4.9.5 电子认证服务机构处理撤销请求的时限

群盾CA从收到证书撤销请求起 24 小时内完成请求的处理。

4.9.6 依赖方检查证书撤销的要求

在具体应用中，依赖方是否检查证书撤销完全取决于应用，如果进行证书的状态检查，必须使用以下两种功能之一进行证书的状态查询：

1)CRL查询：利用证书中标识的CRL地址，查询并下载CRL到本地，进行证书状态的检验。

2)在线证书状态查询(OCSP)：服务系统接受证书状态查询请求，从目录服务器中查询证书的状态，查询结果经过签名后，返回给请求者。

注意：依赖方要验证CRL的可靠性和完整性，确保是经群盾CA发布并且签名的。

4.9.7 CRL的颁发频率

群盾CA将通过证书撤销列表在24小时内公布被撤销的证书，特殊紧急情况下可以立即签发公布。。

4.9.8 CRL发布的最长滞后时间

一个证书从它被撤销到它被发布到CRL上的滞后时间不超过24小时。

4.9.9 在线状态查询的可用性

群盾CA提供7*24小时的在线证书状态查询服务（OCSP），以供安全保障要求高的应用使用。

4.9.10 在线状态查询要求

对于安全保障要求高并且完全依赖证书进行身份鉴别与授权的应用，信赖方在信赖一个证书前必须通过证书状态在线查询检查该证书的状态。

4.9.11 撤销信息发布的其他形式

群盾CA网站（http://www.trondun.com）提供CRL文件下载工具。

4.9.12 密钥损害的特别要求

群盾CA所有订户在发现证书密钥受到损害时，应立即通知群盾CA撤销证书。

4.9.13 证书挂起的情形

群盾CA目前无此业务。

4.10. 证书状态服务

4.10.1 操作特点

群盾CA通过CRL、OCSP提供证书状态服务。

群盾CA提供的证书状态查询以网络服务的形式，让信赖方能够随时查询、下载。CRL的发布频率和延迟必须符合§4.8.7、§4.8.8。OCSP应能立即反映证书的当前状态。证书状态服务的提供使用标准、通用的方式。对服务请求有合理的响应时间和并发处理能力。

4.10.2 服务可用性

CRL、OCSP提供7×24小时的证书状态查询服务。即在网络允许的情况下，订户能够实时获得证书状态查询服务。

4.10.3 可选特征

根据请求者的要求，在请求者支付相关费用后，群盾CA可以提供以下通知服务：

收到证书主题的电子签名消息的接受者要求，确认该证书是否已被撤销；

提供通知服务，当指定的证书被撤销时，群盾CA将通知请求该项服务的请求者。

4.11. 订购结束

订购结束是指当证书有效期满或证书撤销后，该证书的服务时间结束。

订购结束包含以下两种情况：

1)证书有效期满，订户不再延长证书使用期或者不再重新申请证书时，订户可以终止订购；

2)在证书有效期内，证书被撤销后，即订购结束。

4.12. 密钥生成、备份与恢复

4.12.1 密钥生成、备份与恢复的策略和行为

证书订户的加密密钥由群盾密钥管理中心（KMC）托管备份，当证书订户本人、国家执法机关、司法机关或其他管理部门因管理需要提出恢复加密密钥时，由群盾CA通过相应程序从KMC为其取得相应的加密密钥。加密密钥被加密存放在KMC管理中心。

为保证订户签名私钥的安全性，群盾CA不保管签名私钥。因此，要求订户妥善保管签名私钥。由于签名私钥遗失所造成的损失由证书订户自己承担，群盾CA不负责。

4.12.2 会话密钥的封装与恢复的策略和行为

非对称算法组织数字信封的方式来封装会话密钥。数字信封使用信息接受者的公钥对会话密钥加密，接受者用自己的私钥解开并恢复会话密钥。

5. 电子认证服务机构设施、管理和操作控制

5.1. 物理控制

群盾CA电子认证服务机构的物理环境满足以下安全要求：

1）防止物理非法进入

群盾CA通过入侵报警、视频监控等安防设施对定义的十一层管理区域进行实时监测，并建立完善的安全管理制度，保护群盾CA的电子认证服

务设施。

2) 防止未授权访问

群盾CA通过门禁系统和权限分割的管理模式，确保不发生未经过授权或越权的区域访问。

5.1.1 场地位置与建筑

群盾CA电子认证服务业务的运行场地位于北京市海淀区北清路中关村壹号天地融大厦。

核心机房：

群盾CA的功能区域划分为以下区域：办公区、安全监控室、制证室、CA管理区、CA服务区、CA核心区。

群盾CA的核心机房安全区域采用了六面钢板及专用屏蔽门进行屏蔽处理，以防止电磁泄漏，增加系统的安全性，该区域内放置保险柜。CA其他区域采用实墙进行隔离，便于维护管理。

CA出入门由门禁出入卡系统进行控制，并在安全区采用指纹识别与密码结合的方式实施。每个区域都安装视频监控系统、防侵入报警系统、机械组合锁等装置。

其他功能区域：

包括UPS配电间、监控室、机房中心通道、办公区域、制证中心等。机房中心通道与办公区域连接部位采用玻璃门，并且由门禁出入系统进行管理。UPS配电间、监控室采用实墙隔断，监控室需要通过门禁出入卡系统才能进入房间。

5.1.2 物理访问

群盾CA的核心机房和各功能区域的访问控制系统是与控制各区域进出的门禁系统相结合的，并实现了以下安全功能：

1) 进出每一区域的门都有记录作为审计依据；

2) 核心机房的安全区域采用密码和指纹验证的结合方式控制；

3) 其他功能区域只采用身份鉴别卡控制门的进出；

4) 授权人员进出每一道门都会有时间记录；

5) 只有相关授权人员使用授权口令才可以登录访问物理设备；

6) 根据操作性质及安全性的不同，物理设备设置多种权限级别账户（组）对人员进行访问控制，确保物理设备系统安全性；

7) 涉及物理设备密码及重大系统操作的，必须3人以上同时在场才可操作；

8) 高安全级别的重要系统设备的操作与维修，必须在机房内多人现场监控下现场完成且有相关记录。

5.1.3 电力与空调

机房电源供电系统包括机房区的动力、照明、监控、通讯、维护等用电系统，按负荷性质分为计算机设备负荷和辅助设备负荷，计算机设备和动力设备分开供电。供配电系统的组成包括配电柜、动力线缆、线槽及插座、接地防雷、照明箱及灯具、应急灯、照明线管等。计算机设备专用配电柜和辅助设备配电柜独立设置。

使用不间断电源(UPS)来保证供电的稳定性和可靠性。采用双电源，

在单路电源损坏时，可以自动切换，维持系统正常运转，门禁系统、视频监控系统和入侵检测报警系统均接入UPS，可保证8小时不间断供电。

根据机房环境及设计规范要求，主机房和基本工作间，均设置了空气调节系统。空调系统使用中央空调。其组成包括精密空调、通风管路、新风系统。

群盾CA的要求参照电信设施管理的规定，而且每年对物理系统的安全性进行检查。

5.1.4 水患防治

机房内无渗水、漏水现象，主要设备采用专用的防水插座，并采取必要措施防止下雨或水管破损，造成天花板漏水、地板渗水和空调漏水等现象。

群盾CA的系统有充分保障，能够防止水侵蚀。

目前机房空调间做了严格防水处理。

5.1.5 火灾预防和保护

群盾CA的机房建设耐火等级符合GBJ45《高层民用建筑设计防火规范》中规定的二级耐火等级。

符合现行国家有关消防标准规范，为保障建筑内部装修的消防安全，贯彻“预防为主，防消结合”的消防工作方针，防止和减少建筑物火灾的危害。

消防自动报警系统，包括烟感、温感探测器等消防设备，并与大楼

的消防报警系统互连。

烟感及温感探测器按国内规范布置。

消防自动报警系统会作出消防联动控制，火灾报警后，系统通过设置在机房的温感和烟感采集消防数据，同时供系统实时处理用户火灾自动报警终端的报警数据和系统运行状态数据。系统管理分手动模式和自动模式两种，实现网络系统实时检测、监测和系统的手动、自动控制模式的设定，并完成了系统设计的有关各种联动动作。

CA机房消防报警系统建设根据《卤代烷1211灭火系统设计规范(GBJ110-87)》，采用江西兴安生产的七氟丙烷自动灭火系统，型号：CQQ90。北京群盾科技有限公司中心机房自动消防系统已经通过了消防部门的检测。

5.1.6 介质存储

群盾CA对存储有各类软件、运营数据和记录的各类介质妥善控制和保管。这些介质都会被存放在结构坚固的保险柜中，并放置在天地融大楼，对存放的地点设置安全保护，防止诸如潮湿、磁力、灾害以及人为可能造成的危害和破坏，同时记录介质的使用、库存、维修、销毁事件等。群盾对介质的存储地点进行监控，并且只有授权人员才能进入。

5.1.7 废物处理

当群盾CA存档的敏感数据或密钥已不再需要或存档的期限已满时，应当将这些数据进行销毁。写在纸张之上的，必须切碎或烧毁。如果保

存在磁盘中，应多次重写覆盖磁盘的存储区域，其他介质以不可恢复原则进行相应的销毁处理。

5.1.8 异地备份

群盾CA办公区位于北京市海淀区北清路中关村壹号天地融大厦11楼数字认证机房，异地备份位于天津市武清开发区泉达路20号，业务数据光盘、归档电子记录每个月进行备份保存。

5.2. 程序控制

5.2.1 可信角色

所有涉及CA及其RA业务操作和维护管理的人员，可能是群盾CA雇员或代理人员、承包人员、顾问等，都属于可信人员。这些可信人员担任的角色包括但不限于以下部分：

1.RA业务操作员

2.RA业务管理员

3.RA超级管理员

4.CA业务操作员

5.CA业务管理员

6.CA超级管理员

7.密钥管理员

8.安全审计员

9.业务办理服务人员

10. 系统维护人员

11. 数据库维护人员

12. 物理环境维护人员

13. 网络维护人员

5.2.2 角色要求人数

群盾CA对于涉及敏感信息的操作任务，要求采取三人控制策略，并为担任该任务角色至少配置3人。某些涉及敏感信息的区域的进入采取双人控制策略；核心秘密（如CA根密钥）分管者和操作的物理访问控制者由不同的人员担任角色。

5.2.3 可信角色鉴别

所有担任可信角色的人员需持有经授权的智能门禁卡（或密码+指纹）进入相应的活动区域，或在有进入该区域权限的可信人员的陪同下进入,并持有经授权的电子密匙和证书进入系统进行相应业务的操作和管理。

5.2.4 职责需分离的角色

群盾CA及群盾CA的注册机构建立并执行严格的控制流程，根据工作要求和工作安排采取职责分离措施，建立互相牵制、互相监督的安全机制，确保由多名可信人员共同完成敏感操作。群盾CA进行职责分离的角色，包括但不限于下列人员：

1) 证书业务受理；

2）证书或CRL签发；

3）系统工程与维护；

4）CA密钥管理；

5）安全审计。

5.3. 人员控制

5.3.1 人员资格要求

群盾CA在录用担任可信角色的人员之前，除需满足一般的技能和经验要求外，必须按群盾CA可信人员背景调查管理的相关操作指南要求，对录用岗位的可信人员进行对应调查级别的背景调查，符合要求方予录用。可信人员背景调查至少包括以下方面：

1）学历、学位、职称

2）过往的就业情况

对于较高可信等级的调查可能还包括社会关系、奖惩记录、犯罪记录、社会保险记录、交通违章记录、征信记录等。

5.3.2 背景审查程序

群盾CA制定了严格的员工背景审查程序，与有关的政府部门和调查机构合作，完成对群盾CA可信任员工的背景调查。

身份背景调查过程中，存在（但不限于）下列情形之一，不得通过可信审查：

1）伪造相关证件材料的

2）伪造工作经历及工作证明人虚假的

3）虚假声称具有某种技能、能力的证件

4）以往工作中存在重大不诚实行为的

5）有犯罪记录的。

5.3.3 培训要求

群盾CA对群盾CA员工进行以下内容的综合性培训：

1）群盾CA安全原则和机制；

2）群盾CA使用的软件介绍；

3）群盾CA操作的系统和网络；

4）岗位职责；

5）群盾CA政策、标准和程序；

6）相关法律、仲裁规则、管理办法等。

针对关键岗位员工进行相关职责、安全机制、工作操作说明等方面内容的培训。

5.3.4 再培训周期和要求

根据群盾CA策略调整、系统更新等情况，群盾CA将对员工进行继续培训，以适应新的变化。对于公司安全管理策略，每年对员工进行一次以上的培训，对于相关业务技能培训应每年进行一次以上的业务技能培训。

5.3.5 工作轮换周期和顺序

根据岗位人员和业务上的实际情况内部自行安排。

5.3.6 对未授权行为的处罚

当群盾CA员工进行了未授权或越权操作，群盾CA在确认后将立即中止该员工进入群盾CA证书服务体系，根据情节严重程度实施包括提交司法机关处理等措施。

一旦发现上述情况，群盾CA立即作废或终止该人员的电子密匙。

5.3.7 独立合约人的要求

群盾CA的独立合约人及顾问执行与普通员工一致的可信资格确认，此外独立合约人及顾问进入关键区域必须有专人的陪同与监督。

5.3.8 提供给员工的文档

在培训或再培训期间，群盾CA提供给员工的培训文档包括（但不限于）以下几类：

1)员工手册；

2)电子认证业务规则；

3)岗位说明书；

4)安全管理制度等。

5.4. 审计日志程序

5.4.1 记录事件的类型

群盾CA的CA和RA运行系统，记录所有与系统相关的事件，以备审查。这些记录，无论是纸质或电子文档形式，都包含事件日期、事件的内容、事件的发生时间段、事件相关的实体等。

群盾CA应记录的内容包括（但不限于）：

1）系统安全事件，包括： CA系统、RA系统和其他服务系统的活动，系统崩溃，硬件故障和其他异常。

2）电子认证服务系统操作事件，包括系统的启动和关闭。

3）认证机构设施的访问，包括授权人员进出认证机构设施、非授权人员进入认证机构设施及陪同人和安全存储设施的访问。

4）证书生命周期相关事件。

5.4.2 处理或归档日志的周期

对于CA和订户证书生命周期内的管理事件日志，群盾CA将一个季度进行一次内部检查、审计。

系统安全事件和系统操作事件日志群盾CA将每月进行一次检查、处理。

物理设施的访问日志群盾CA将每季度进行一次检查、处理。

5.4.3 审计日志的保存期限

群盾CA在本地审计记录至少保存三个月，与证书相关的信息，保存

证书失效后五年。

5.4.4 审计日志的保护

群盾CA执行严格的管理，确保只有群盾CA授权的人员才能对审查日志进行相应操作。日志处于严格的保护状态，严禁在未授权的情况下被访问、阅读、修改和删除等操作，另外对日志要进行异地备份。审计日志的制作和访问进行岗位分离。

群盾CA将审计日志存储到光盘中，并存放到异地，实行安全保管。

5.4.5 审计日志备份程序

群盾CA保证所有的审查记录和审查总结都按照群盾CA备份标准和程序进行备份。

审计文档由管理员按季度进行归档，所有档案安全存放在文档库内。

5.4.6 审计日志收集系统

审计日志收集系统涉及：

证书管理系统；

证书签发系统；

证书目录系统；

远程通信系统；

证书受理系统；

网站、数据库安全管理系统；

其他需要审计的系统。

群盾CA使用审计工具满足对上述系统审计的各项要求。

5.4.7 对导致事件实体的通告

群盾CA发现被攻击现象，将记录攻击者的行为，在法律许可的范围内追溯攻击者，群盾CA保留采取相应对策措施的权利。根据攻击者的行为采取包括切断对攻击者已经开放的服务、递交司法部门处理等措施。

群盾CA有权决定是否对导致事件的实体进行通告。

5.4.8 脆弱性评估

群盾CA每年对系统进行脆弱性评估，以降低系统运行的风险。

5.5. 记录归档

5.5.1 归档记录的类型

群盾CA按照制度和流程定期对电子生成和（或者）手工生成的重要数据定期存档。存档的内容包括订户资料、电子认证系统签发的系统证书和订户证书、证书撤销列表CRL、电子认证系统维护操作记录、可信人员进出机房操作记录、外来人员进出记录、数据备份记录、涉及电子认证安全的事件记录及审计数据等。

5.5.2 归档记录的保存期限

所有归档记录的保存期为证书失效后五年。

5.5.3 归档文件的保护

存档内容既有物理安全措施的保证，也有密码技术的保证。只有经过授权的工作人员按照特定的安全方式才能查询。群盾CA保护相关的档案内容，免遭恶劣环境的威胁，如温度、湿度和强磁力等的破坏。

5.5.4 归档文件的备份程序

所有存档的文件和数据库除了保存在群盾CA的存储库，还在异地保存其备份。存档的数据库一般采取物理或逻辑隔离的方式，与外界不发生信息交互。只有被授权的工作人员或在其监督的情况下，才能对档案进行读取操作。群盾CA在安全机制上保证禁止对档案及其备份进行删除、修改等操作。

5.5.5 记录时间戳要求

所有记录都要在存档时加具体准确的时间标识以表明存档时间。

5.5.6 归档收集系统

群盾CA的档案收集系统由人工操作和自动操作两部分组成。

5.5.7 获得和检验归档信息的程序

只有被授权的可信人员能够访问归档记录。所有记录被访问后，需验证其完整性。此外，群盾CA每年验证存档信息的完整性。

5.6. 电子认证服务机构密钥更替

在CA的密钥对遭受攻击或因为密钥生命期而需要更新密钥对的情况下，由安全中心授权，所有密钥管理员在场，共同启动密钥管理程序，执行密钥更新指令，硬件加密设备重新生成根密钥。密钥更换及自签名证书按照规定报告上级管理机构。

5.7. 损害和灾难恢复

5.7.1 事故和损害处理程序

群盾CA已制定各种应急处理方案，规定了相应的事故和损害处理程序，应急处理方案包括：

1）认证系统应急方案；

2）电力系统应急方案；

3）消防应急方案；

4）网络与信息系统应急方案；

5）安全事故应急处理方案等。

涉及电子认证机构的重大事故应按照规定及时上报管理机构。

5.7.2 计算资源、软件和/或数据被破坏

群盾CA对业务系统及其他重要系统的资源、软件和/或数据进行了备份，并制定了相应的应急处理流程。当出现计算机资源、软件或数据的损坏时，能在最短的时间内恢复被损害的资源、软件和/或数据。

5.7.3 实体私钥损害处理程序

对于实体私钥的损害，群盾CA有如下处理要求和程序：

1）当证书订户发现实体证书私钥损害时，订户必须立即停止使用其私钥，并立即通知群盾CA或注册机构撤销其证书。群盾CA按《群盾CA CPS》§4.9发布证书撤销信息。

2）当群盾CA或注册机构发现证书订户的实体私钥受到损害时，群盾CA或注册机构将立即撤销证书，并通知证书订户，订户必须立即停止使用其私钥。群盾CA按《群盾CA CPS》§4.9 发布证书撤销信息。

3）当群盾CA的证书出现私钥损害时，群盾CA将立即撤销CA证书并及时通过广达的途径通知依赖方，然后生成新的CA密钥对、签发新的CA证书。

5.7.4 灾难后的业务连续性能力

针对证书系统的核心业务系统，证书签发系统和证书接口系统采用双机冷备方式；对核心数据库，证书管理系统数据库采用双机热备方式来确保证书系统的高可靠性和可用性。

除非物理场地出现了毁灭性的、无法恢复的灾难，群盾CA能够在出现灾难后最短时间内恢复其业务能力。

5.8. 电子认证服务机构或注册机构的终止

因各种情况，群盾CA需要终止运营时，将按照相关法律规定的步骤终止运营，并按照相关法律法规的要求进行档案和证书的存档。

群盾CA在终止服务九十日前，就业务承接及其他有关事项通知有关各方，包括但不限于群盾CA授权的注册机构和订户等。

在终止服务六十日前向工业和信息化部报告，按照相关法律规定的步骤进行操作。

群盾CA采用以下措施终止业务：

1)起草群盾CA终止业务声明；

2)停止认证中心所有业务；

3)处理加密密钥；

4)处理和存档敏感文件；

5)清除主机硬件；

6)管理群盾CA系统管理员和安全官员；

7)通知与群盾CA终止运营相关的实体。

根据群盾CA与注册机构签订的运营协议终止注册机构的业务。

6. 认证系统技术安全控制

6.1. 密钥对的生成和安装

由于密钥对是安全机制的关键，所以在电子认证业务规则中制定了相应的规定，通过物理安全控制和密钥安全存储控制来确保密钥对的产生、传送、安装等过程中符合保密性、完整性和不可否认性的需求。

6.1.1 密钥对的生成

加密密钥对是由中华人民共和国国家密码管理局许可的、群盾CA数字证书签发系统支持的加密机设备生成的，由群盾CA所属的KMC控制管理。

签名密钥对是由客户端产生，证书订户可使用群盾CA数字证书签发系统支持的介质生成签名密钥对。签名密钥存储在介质中不可导出，保证群盾CA无法复制签名密钥对。

群盾CA支持多种介质，如智能密码钥匙、智能IC卡等。群盾CA可根据证书订户要求或自身选择签名密钥对生成介质。

服务器证书的密钥对由订户自己产生，订户应妥善保管。

群盾CA通过物理安全控制和密钥安全存储控制，在技术、流程和管理上保证密钥对产生的安全性。

6.1.2 加密私钥传送给订户

订户自己生成的密钥对的情况下，不需要将私钥传给订户。

证书订户的加密私钥是在KMC产生的，该私钥只保存在KMC。在加密私钥从KMC到订户的传递时，采用国家密码管理局许可的对称密钥算法加密，群盾CA无法获得，这样就保证了证书订户加密私钥的安全。

6.1.3 公钥传送给证书签发机构

群盾CA从KMC取得订户加密公钥后为其签发证书，在此过程中采用国家密码管理局许可的对称密钥算法加密，保证了传输中密钥的安全。

自生成密钥对证书订户向群盾CA提交证书申请时，该请求信息内的公钥，使用安全通道保证信息的机密性和完整性。

6.1.4 电子认证服务机构公钥传送给依赖方

群盾CA的根公钥包含在群盾CA自签发的根证书中。证书订户可以从群盾CA 的网站（http://www.trondun.com）上下载群盾CA根证书，也可以由群盾CA通过目录系统、业务系统的安装、电子邮件和软件绑定等方式提供给依赖方。

6.1.5 密钥的长度

为了保证加密/解密的安全性，群盾CA所使用的密钥对长度

为1024位。如果国家法律法规、政府主管机构等对密钥长度有明确的规范和要求，群盾CA将会完全遵从。

6.1.6 公钥参数的生成和质量检查

公钥参数由国家密码管理局许可、群盾CA数字证书签发系统支持的硬件产生；质量检查由国家密码管理局具体实施。

6.1.7 密钥使用用途

在群盾CA证书服务体系中的密钥用途和证书类型紧密相关，被分为签名和加密两大类。

1）群盾CA的签名密钥用于签发RA证书和证书撤销列表（CRL）；

2）RA的签名密钥用于确认RA所做的审批证书等操作；

3）订户的签名密钥用于提供网络安全服务，如信息在传输过程中不被篡改、接收方能够通过数字证书来确认发送方的身份、发送方对于自己发送的信息不能抵赖等；

4）订户加密密钥用于对需在网络上传送的信息进行加密，保证信息除发送方和接受方外不被其他人窃取、篡改。

更多与协议和应用相关的密钥使用限制请参阅X.509标准中的密钥用途扩展域。

6.2. 私钥保护和密码模块工程控制

6.2.1 密码模块标准和控制

群盾CA使用国家密码管理局许可的产品，密码模块的标准符合国家规定的要求。

6.2.2 私钥多人控制（m选n）

群盾CA采用多人控制策略激活、使用、备份、停止和恢复群盾CA的签名密钥，采取5个管理人员中至少3个在场才可进行操作的原则。

6.2.3 私钥托管

KMC可以根据客户和法律的需要，对加密密钥进行托管。签名私钥由订户自己保管，以保证其不可否认性。

6.2.4 私钥备份

群盾CA对其签名私钥通过专门的备份加密卡进行备份，私钥的备份采用多人控制策略。

KMC备份托管的订户加密私钥，确保加密私钥的安全。

6.2.5 私钥归档

KMC提供过期的托管私钥的存档服务；保存期为五年。当私钥过了保存期，将依据相关规定对其进行销毁。

6.2.6 私钥导入、导出密码模块

在群盾CA业务系统中，可以把订户的私钥导入指定的密码模块中。私钥无法从硬件密码模块中导出，必须通过密码验证之后，才可能使用存储在密码模块中的私钥进行加解密操作。

群盾CA的根CA私钥在硬件密码模块上生成，保存和使用。群盾CA对根CA私钥进行严格的密钥管理和备份、恢复控制，有效防止了根CA私钥的丢失、被窃、修改、非授权的泄露、非授权的使用。

6.2.7 私钥在密码模块的存储

群盾CA私钥以加密的形式存放在硬件密码设备中，并在该设备中使用。

6.2.8 激活私钥的方法

CA私钥存放在硬件密码设备中，具有激活私钥权限的管理员使用含有自己的身份标识的智能卡登录，启动密钥管理程序，进行激活私钥的操作，需要半数以上的管理员同时在场。

6.2.9 解除私钥激活状态的方法

对于CA私钥，具有解除私钥激活状态权限的管理员使用含有自己的身份的智能卡登录，启动密钥管理程序，进行解除私钥的

操作，需要半数以上的管理员同时在声

6.2.10 销毁私钥的方法

对于私钥，具有销毁密钥权限的管理员使用含有自己的身份的智能IC卡登录，启动密钥管理程序，进行销毁密钥的操作，需要半数以上的管理员同时在场。

6.2.11 密码模块的评估

群盾CA使用国家密码主管部门批准和许可的密码产品。

6.3. 密钥对管理的其他方面

6.3.1 公钥归档

订户证书中的公钥包括签名证书中的公钥和加密证书中的公钥。它们由群盾CA和KMC定期归档。

6.3.2 证书操作期和密钥对使用期限

所有订户证书的有效期与其对应的密钥对的有效期相关但却有所不同。

对于签名用途的证书，其私钥只能在证书有效期内才可以用于数字签名，私钥的使用不超过证书有效期。但是，为了保证证书有效期内的签名可以验证，公钥的使用可以在证书有效期之外，直到私钥受损害或密钥对存在被破解的风险，如加密算法被破解。当私钥受到损害或密钥存在被破解的风险后，签名证书的

公钥仍然可以用于验证数字签名，但这种验证在法律上不一定有效。

对于加密用途的证书，其公钥只能在证书有效期内才可以用于加密信息，公钥的使用不超过证书有效期限。但是，为了保证在证书有效期内加密的信息可以解开，私钥的使用期限可以在证书的有效期限之外。

对于身份鉴别用途的证书，其私钥和公钥只能在证书有效期内可以使用。

当一个证书有多个用途时，公钥和私钥的使用期限是以上情况的组合。

6.4. 激活数据

6.4.1 激活数据的产生和安装

群盾CA将订户证书的私钥保存在USB Key或其它安全介质中，需要用户授权，私钥才能被激活使用。

群盾CA所签发的服务器类证书，证书的私钥由专有的密码模块提供和保存，当服务程序要加载私钥时需求通过保护口令的验证才能访问密码模块中的私钥。

6.4.2 激活数据的保护

通用证书存储介质的PIN值用密码信封中的密码进行保护。

如果证书订户使用口令或PIN码保护私钥，订户应妥善保管

好其口令或PIN码，防止泄露或窃取。

6.4.3 激活数据的其他方面

拥有证书介质并知道证书介质的PIN值时才能激活证书存储介质，进而使用私钥。

当订户证书私钥的激活数据不需要时应该销毁，订户应该确保无法通过残余信息、介质直接或间接恢复激活数据的部分或全部，比如记录有口令的纸页必须粉碎。

6.5. 计算机安全控制

6.5.1 特别的计算机安全技术要求

群盾CA的数字证书签发系统的数据文件和设备由群盾CA系统管理员维护，未经群盾CA管理员授权，其它人员不能操作和控制群盾CA系统；其它普通订户无系统账号和密码。群盾CA系统部署在多级不同厂家的防火墙之内，确保系统网络安全。群盾CA系统密码有最小密码长度要求，而且必须符合复杂度要求，群盾CA系统管理员定期更改系统密码。

6.5.2 计算机安全评估

群盾CA的CA系统及其运营环境通过了中国国家信息安全测评认证中心的运营系统安全测评。

群盾CA根据法律法规和主管部门的规定，按照国家计算机安

全等级的要求，实现安全等级制度。

6.6. 生命周期技术控制

6.6.1 系统开发控制

系统开发采用先进的安全控制理念，同时应兼顾开发环境的安全、开发人员的安全、产品维护期的配置管理安全。系统设计和开发运用软件工程的方法，做到系统的模块化和层次化，系统的容错设计采用多路并发容错方式，确保系统在出错的时候尽可能不停止服务。

6.6.2 安全管理控制

群盾CA的配置以及任何修改和升级都会记录在案并进行控制，并且群盾CA采取一种灵活的管理体系来控制和监视系统的配置，以防止未授权的修改。

认证系统只开放与业务相关的功能，只有群盾CA授权的员工能够进入群盾CA的系统或设备。

6.6.3 生命周期的安全控制

群盾CA的证书认证系统在系统设计过程中充分进行了安全性考虑，在开发过程中有严格的流程进行代码安全管理，在开发完成后进行了严格的安全测试，在正式使用前通过了国家有关部门的系统安全性审查和技术鉴定。

6.7. 网络的安全控制

系统网络安全的主要目标是保障网络基础设施、主机系统、应用系统及数据库运行的安全。群盾CA采取多层防火墙、病毒防治、入侵检测、漏洞扫描、数据备份、灾难恢复等安全防护措施。

6.8. 时间戳

目前未提供时间戳服务。

7. 证书、证书撤销列表和在线证书状态协议

7.1. 证书

群盾CA签发的证书均符合X.509 V3证书格式，遵循RFC3280标准。

7.1.1 版本号

X.509 V3

7.1.2 证书标准项及扩展项

证书标准项：

1) 证书版本号（Version）

指明X.509证书的根式版本，值为V3。

2) 证书序列号（SerialNumber）

指唯一标识该证书的一组32位字符。

3) 证书签名标识符（Signature）

指定签发证书时所使用的签名算法。

4) 签发机构名（Issuer）

用来标识签发证书的CA的 DN名字。

CN = QDCA Root Authority

C = CN

5) 证书有效期（Validity）

指证书的起止时间。

6) 主题（Subject）

指为证书订户申请证书时所填写的申请信息。即订户的甄别名。详细请参看第3.1节。

7) 公钥（subjectPublicKeyInfo）

证书持有者公开密钥信息域包含两个重要信息：证书持有者的公开密钥的值；公开密钥使用的算法标识符。

8) 微缩图算法

证书内容的签名算法。

9) 微缩图

证书内容的签名值。证书扩展项：

10) 授权密钥标识符

授权密钥标识符与验证签名的公开密钥相联系。群盾CA根证书公钥与此标识符相联系。

11) 主题密钥标识符

通过主体密钥标识符识别相对应证书的公钥。

12) 密钥用法

指定各种密钥的用法：电子签名，不可抵赖，密钥加密，数据加密，密钥协议，验证证书签名，验证CRL签名，只加密，只解密，只签名。

13) 密钥扩展使用

暂无。

14) 证书策略

暂无。

15) 基本限制

用于鉴别证书持有者身份，如最终订户等。

16) CRL发布点

由群盾CA定义的CRL发布点。如：

Directory Address：

CN=QDCA SM2 CA，OU=QDCA，O=群盾科技，L=北京市，S=北京市，C=CN

7.1.3 算法对象标识符

群盾CA签发的证书按照RFC 3280标准。用国密sm2算法签名。

7.1.4 名称形式

群盾CA签发证书的甄别名符合 X.500关于甄别名的规定。详情参见§3.1内容。

7.1.5 名称限制

订户在证书中的名称可以是假名，但不能使用匿名，并在群盾CA的数据库中记录订户的相关信息。群盾CA可以按照一定的规则为订户指定特殊名称，并且能够把该类特殊的名称与一个确定的实体（个人、单位或设备）唯一联系起来。

7.1.6 证书策略对象标识符

没有定义。

7.1.7 策略限制扩展项的用法

没有使用。

7.1.8 策略限定符的语法和语义

没有规定。

7.1.9 关键证书策略扩展项的处理规则

与X.509和PKI相关规定一致。

7.2. 证书撤销列表

群盾CA定期签发证书撤销列表（CRL），其所签发的CRL遵循RFC3280标准。

7.2.1 版本号

采用X.509 V2格式。

7.2.2 CRL和CRL条目扩展项

与X.509和PKI规定一致。

1）版本号：用来指定CRL的版本信息。

2）签名算法：群盾CA采用sm2、sm3、sm4算法。

3）颁发者：指定签发机构的DN名。

4）生效时间：指定一个日期/时间值，用以表明本CRL发布的时间。

5）下次更新时间：指定一个日期/时间值，用以表明下一次CRL将要发布的时间。

6）撤销证书列表：指定已经撤销或挂起的证书列表。本列表中含有证书的序列号和证书被撤销的日期和时间。

7）颁发机构密钥标识符：本项标识用来验证在CRL上签名的公开密钥。

8）扩展

7.3. 在线证书状态协议

RFC2560中定义了在线证书状态协议（Online Certificate Status Protocol, OCSP）,它克服了基于CRL的撤消方案的局限性，并且为证书状态查询提供即时的最新响应。

7.3.1 版本号

OCSP：V1。

7.3.2 OCSP 扩展项

与RFC2560一致。

8. 电子认证服务机构审计和其他评估

8.1. 评估的频率或情形

群盾CA需对群盾CA的关联单位（包含群盾CA授权的注册机构、注册分支机构、受理点等证书体系成员）所有的流程和操作进行审计，检验其是否符合本电子认证业务规则和相应的证书政策的规定，其频率可由群盾CA决定或由法律制定的监管机构决定。

根据《中华人民共和国电子签名法》、《电子认证服务管理办法》等的要求，每年一次接受上级主管部门的合规性审计。

根据审计结果，需要整改后复审的，应接受复审。

8.2. 评估者的资质

对群盾CA实施规范审计的第三方所具有的资质和经验必须符合监管法律和行业准则规定的要求，包括：

1) 必须是经许可的、有营业执照的、具有计算机安全专门技术知识的的审计人员或审计评估机构，且在业界享有良好的声誉；

2) 了解计算机信息安全体系、通信网络安全要求、PKI技术、标准和操作；

3) 具备检查系统运行性能的专业技术和工具。

8.3. 评估者与被评估者之间的关系

对群盾CA进行审计的第三方，必须是一个独立于群盾CA的合法审计实体。群盾CA内部审计员不能与系统管理员、业务管理员、业务操作员等岗位重叠。

8.4. 评估内容

审计工作包括：

1) 安全策略是否得到充分实施；

2) 运营工作流程和制度是否严格遵守；

3) 电子认证业务规范是否符合证书策略的要求；

4) 是否严格按照本CPS、业务规范和安全要求开展业务；

5) 各种日志、记录是否完整，是否存在问题；

6) 是否其它可能存在的安全风险；

7) 群盾CA支持的证书认证操作规程是否完全与本电子认证业务规则表达一致，包括群盾CA的技术、手续和员工的相关管理政策和电子认证业务规则；

8) 群盾CA是否实施了相关技术、管理、相关政策和电子认证业务规则；

9) 审计者或群盾CA认为有必要审计的其他方面。

8.5. 对问题与不足采取的措施

如果在审计过程中发现执行有不足之处，由安全策略管理委员会负责监督这些问题的责任职能部门进行业务改进和完善的情况，完成对评估结果的改进后，各职能部门必须向安全中心提交业务改进工作总结报告。

如果在外部评估过程中发现执行有不足之处，群盾CA必须根据评估的结果检查缺失和不足，根据提出的整改要求，提交修改和预防措施以及整改方案，并接受对整改方案的审查，以及对整改情况的再次评估。

8.6. 评估结果的传达与发布

除非法律明确要求，群盾CA一般不公开审计结果。在必要的

情况下，群盾CA 可依照与关联单位（例如注册机构、注册分支机构、受理点）签订的协议中有关规定，向关联单位通知审计结果。

9. 法律责任和其他业务条款

9.1. 费用

9.1.1 证书签发和更新费用

根据群盾CA的价目确定。

9.1.2 证书查询费用

群盾CA目前不对证书查询收取专门的费用。

9.1.3 证书撤销或状态信息的查询费用

证书撤销列表（CRL）的获取不收取任何费用。群盾CA有可能根据需要将OCSP 服务作为增值服务收取费用。

9.1.4 其他服务费用

根据群盾CA的价目确定。

9.1.5 退款策略

如果由于群盾CA违背了本证书策略所规定的责任，造成订户合同无法履行、订户证书无法使用，群盾CA会对订户证书进行撤销并将订户为申请证书所支付的费用退还给订户。

9.2. 财务责任

9.2.1 保险范围

群盾CA根据业务发展情况和国内保险公司的业务开展情况决定其投保策略。

9.2.2 其它资产

群盾CA确保具有足够的财务实力来维持其正常经营并保证相应义务的履行，并合理地承担对订户及对依赖方的责任。

此要求对证书订户同样适用。

9.2.3 对最终实体的保险或担保范畴

如果群盾CA根据司法判定须承担赔偿和补偿责任的，群盾CA将按照相关仲裁机构的裁定或法院的判决承担相应的赔偿责任。

9.3. 业务信息保密

群盾CA有专门的信息保密制度，保护自身和订户的敏感信息、商业秘密。

9.3.1 保密信息范围

群盾CA保密的信息包括但不限于以下内容：

1、群盾CA与订户之间的协议、资料中未公开的内容等属于保密信息。除非法律明文规定或政府、执法机关等的要求，群盾

CA承诺不对外公布或透露订户证书信息以外的任何其它隐私信息。

2、订户私钥属于机密信息。订户应当根据本CPS的规定妥善保管，如因订户自己泄漏私钥造成的损失，订户应自行承担。

9.3.2 不属于保密的信息

与证书有关的申请流程、手续、申请操作指南等信息是公开的。注册机构在处理申请业务时可以利用这些信息，包括发布上述信息给第三方。

订户数字证书的相关信息可以通过群盾CA目录服务等方式向外公布。

9.3.3 保护保密信息的责任

群盾CA有各种严格的管理制度、流程和技术手段保护机密信息，包括但不限于商业秘密、客户信息等。每个员工都必须接受信息保密方面的培训，并与公司签订保密协议。任何参与方有责任保证不泄露保密信息。

9.4. 个人隐私保密

9.4.1 隐私保密方案

群盾CA制定有隐私保护制度并签定保密协议，保证证书订户的个人信息不被滥用、未授权使用或出售，同时采取必要措施防

止客户资料不被遗失、盗用与篡改。

9.4.2 作为隐私处理的信息

作为隐私处理的信息包括：最终订户注册申请证书中提交的信息，包括联系电话、地址等；订户与群盾CA、注册机构签订的协议。

9.4.3 不被视为隐私的信息

不被认为是隐私信息包括：用来构成证书内容的信息，证书及证书状态。

9.4.4 保护隐私的责任

除非执法、司法方面的强制需要，群盾CA及注册机构在没有获得订户授权的情况下，不会将订户隐私信息透露给第三方。

9.4.5 使用隐私信息的告知与同意

1、订户同意，群盾CA在业务范围内并按照本CPS规定的隐私保护政策使用所获得的任何订户信息，无论是否涉及到隐私，群盾CA均可以不用告知订户。

2、订户同意，在任何法律法规或公共权力部门要求下，群盾CA向特定对象披露隐私信息时，群盾CA均可以不用告知订户。

9.4.6 依法律或行政程序的信息披露

当群盾CA在任何法律、法规或规章条款的要求下，或在司法机关的要求下必须披露本电子认证业务规则中具有保密性质的信息时，群盾CA可以按照法律、法规或规章条款以及司法机关的要求，向执法部门公布相关的保密信息。这种披露不视为违反了保密的要求和义务。

9.4.7 其他信息披露情形

对其他信息的披露受制于法律、订户协议。

9.5. 知识产权

群盾CA保留对《群盾CA CPS》的所有知识产权。

群盾CA保留其签发的证书和证书撤销信息的所有知识产权。任何人可以免费地复制、分发证书和证书撤销列表，只要他们进行完整复制并且证书和证书撤销列表的使用符合相应的依赖方协议。

证书订户保留证书申请中包含的订户拥有的商标、服务标志或商业名称以及签发给该证书订户的证书中的可辨识名的所有权利。

证书所有者拥有其证书相关的密钥对的知识产权。

9.6. 陈述与担保

9.6.1 电子认证服务机构的陈述与担保

除非群盾CA作出特别约定，若本电子认证业务规则的规定与其他群盾CA制定的相关规定、指导方针相互抵触，订户必须接受本电子认证业务规则的约束。在群盾CA与包括订户在内的其他方签订的仅约束签约双方的协议中，对协议中未约定的内容，视为双方均同意按本电子认证业务规则的规定执行；对协议中有不同于本电子认证业务规则内容的约定，按双方协议中约定的内容执行。

群盾CA承担的责任和义务是：

1）保证电子认证服务机构本身使用和发放的公钥算法在现有通常技术条件下不会被攻破；

2）保证群盾CA的签名私钥在群盾CA内部得到安全的存放和保护；

3）群盾CA建立和执行的安全机制符合国家政策的规定。

群盾CA不对由于客观意外或其他不可抗力事件造成的操作失败或延迟承担任何损失、损坏或赔偿责任。这些事件包括劳动纠纷、交易一方故意或无意的行为、罢工、暴动、骚动、战争、火灾、爆炸、地震、水灾或其他大灾难等。

针对上述内容补充解释如下：

第一：除上述所规定的职责条款，群盾CA、群盾CA的服务机

构、群盾CA授权的注册机构、群盾CA的雇员不承担其它任何义务。必须指出，本电子认证业务规则的内容，没有任何信息可以暗示或解释成群盾CA必须承担其它的义务或群盾CA 必须对其行为作出其它的承诺。

第二：在上述内容中所罗列不可抗力的任何情况下，群盾CA由于受到影响，可免除本节所述的责任和相应的证书策略规定的责任和义务。

第三：由于技术的进步与发展，为保证证书的安全性，群盾CA会要求证书持有者及时更换证书以保证群盾CA能更好地履行本节所述之责任。

9.6.2 注册机构的陈述与担保

注册机构必须遵守所有的登记程序和安全保障措施。这些程序和保障由群盾CA决定，并在本电子认证业务规则或相应的注册机构协议中规定，以后群盾CA 可以根据情况修改有关内容，并及时公布。

注册机构必须遵守和符合本电子认证业务规则的条款。具体内容详见第9.6.1条。

9.6.3 订户的陈述与担保

所有的订户必须严格遵守关于证书申请以及私钥的所有权和安全保存相关的程序：

订户在证书申请表上填列的所有声明和信息必须是完整、精确、真实和正确的，可供群盾CA或受理点检查和核实；

订户必须严格遵守和服从电子认证业务规则规定的或者由群盾CA推荐使用的安全措施；

订户需熟悉本电子认证业务规则的条例和与证书相关的证书政策，遵守订户证书使用方面的有关限制；

一旦发生任何可能导致安全性危机的情况，如遗失私钥、遗忘或泄密以及其他情况，订户应采取必要的救济措施，并立刻通知群盾CA或群盾CA授权的注册机构，申请采取挂失、废除等处理措施。

9.6.4 依赖方的陈述与担保

依赖方确认，在任何信赖行为发生之前，阅读了依赖方协议，并评估了在特定应用中信赖证书的适当性，不在证书适用目的以外的应用中信任证书。

9.6.5 其他参与者的陈述与担保

遵守本CPS的所有规定。

9.7. 担保免责

有下列情形之一的，应当免除群盾CA之责任：

订户在申请和使用群盾CA数字证书时，有违反如下义务之一的：

1) 订户应当提供真实、完整、准确的材料和信息，不得提供虚假、无效的材料和信息；

2) 订户应当妥善保管群盾 CA 所签发的数字证书载体和保护 PIN 码，不得泄漏 PIN 码或将数字证书载体随意交付他人；

3) 订户在应用自己的密钥或使用数字证书时，应当使用可依赖的、安全的系统；

4) 订户知悉电子签名制作数据已经失密或者可能已经失密时，应当采取必要的救济措施，及时告知群盾 CA 及相关各方，并终止使用该电子签名制作数据；

5) 订户在使用数字证书时必须遵守国家的法律、法规和行政规章制度，不得将数字证书在群盾 CA 规定使用范围之外的其他任何用途使用；

6) 订户必须在证书有效安全期内使用该证书，不得使用已失密或可能失密、已过有效期、被挂起、被撤销的数字证书。

由于非群盾CA原因造成的设备故障，网络中断导致证书报错，交易中断或其他事故造成的损失，损失方可以追究侵权方责任，群盾CA给予配合，但是群盾CA不向任何方承担赔偿或补偿责任。

由于不可抗力原因而导致数字证书签发错误、延迟、中断、无法签发，或暂停、终止全部或部分证书服务的。本项所规定之“不可抗力”，是指不能预见、不能避免并不能克服的客观情况，包括（但不限于）：自然灾害，包括地震、火山爆发、滑坡、泥石流、雪崩、洪水、台风等；社会异常或者政府行为，包括政府

颁发新的政策、法律和行政法规，或战争、罢工、骚乱等社会异常事件。

群盾CA已谨慎地遵循了国家法律、法规规定的数字证书认证业务规则，而仍有损失产生的。

9.8. 有限责任

在与订户和依赖方签定的协议中，群盾CA对于因订户或依赖方的原因造成的损害不具有赔偿义务。

9.9. 赔偿

对于由如下原因造成的订户或依赖方损失，群盾CA对订户或依赖方进行赔偿：

1）群盾CA在批准证书前没有严格按业务程序确认证书申请，造成证书的错误签发；

2）由于群盾CA的原因，使得证书中出现了错误信息。

在如下情况，订户对自身原因造成的群盾CA、依赖方损失承担责任：

1）订户在证书申请中对事实进行虚假或错误描述；

2）在证书申请中订户没有披露重要的事实，如果这种错误表述或遗漏是因为粗心或故意欺骗任何一方；

3）订户没有使用可信系统保护私钥，或者没有采取必要的注意防止订户私钥的安全损害、丢失、泄漏、修改或非授权的使

用；

4) 订户使用的名字（包括但不限于通用名、域名）破坏或侵犯了第三方的知识产权。

在如下情况，依赖方对自身原因造成的群盾CA损失承担责任：

1) 依赖方没有执行依赖方职责义务；

2) 依赖方在不合理的环境下信赖一个证书；

3) 依赖方没有检查证书状态确定证书是否过期或撤销。

群盾CA只有在其证书有效期限内承担损失损害赔偿，群盾CA承担赔偿责任（法定或约定免责除外）的赔偿限制如下：

1) 群盾CA对任何证书订户、依赖方等实体有关证书赔偿的合计责任限制在不超出下述数量的范围内：

证书类型	赔偿金额上限
自然人证书	800 元 RMB
机构（企业）证书	4000 元 RMB
设备证书	8000 元 RMB

这种赔偿上限可以由群盾CA根据情况重新制定，群盾CA会将重新制定后的情况立刻通知相关当事人。

2) 对于由订户或依赖方的原因造成的损失，群盾CA不承担责任，由订户或依赖方自行承担。

证书订户和依赖方在使用或依赖证书时，若有任何行为或疏漏而导致群盾CA和注册机构产生损失，订户和依赖方应承担赔偿责任。

订户接受证书就表示同意在以下情况下承担赔偿责任：

1）未向注册机构提供真实、完整和准确的信息，而导致群盾CA或有关各方损失。

2）未能保护订户的私钥，或者没有使用必要的防护措施来防止订户的私钥遗失、泄密、被修改或被未经授权的人使用时。

3）在知悉证书密钥已经失密或者可能失密时，未及时告知群盾CA，并未终止该证书，而导致群盾CA或有关各方损失。

4）订户如果向依赖方传递信息时表述有误，而依赖方用证书验证了一个或多个电子签名后理所当然地相信这些表述，订户必须对这种行为的后果负责。

5）证书的非法使用，即违反群盾CA对证书使用的规定，造成了群盾CA或有关各方的利益受到损失。

9.10. 有效期限与终止

9.10.1 有效期限

本CPS自发布之日起生效。

9.10.2 终止

当新版本的CPS生效时或群盾CA终止业务时，旧版本CPS自动终止；当群盾CA中止业务时，群盾CA CPS自动终止。

9.10.3 效力的终止与保留

本CPS终止后，已签发符合本证书策略的证书，效力作用直到证书到期或撤销。

当由于某种原因，如内容修改、与适用法律相冲突，证书策略、电子认证业务规则、订户协议、依赖方协议和其他协议中的某些条款失效后，不影响文件中其他条款的法律效力。

9.11. 对参与者的个别通告与沟通

群盾CA及其注册机构在必要的情况下，如在主动撤销订户证书、发现订户将证书用于规定外用途及订户其他违反订户协议的行为时，会通过适当方式，如电话、电邮、信函、传真等，个别通知订户、依赖方。

9.12. 修订

群盾CA有权在合适的时间修订本电子认证业务规则中任何术语、条件和条款，而且无须预先通知任何一方。

群盾CA有权在群盾CA的自主数据库中设置和公布修改结果，或以其他方式（如修改CPS版本的形式或在网站上）公布。所有的修订在公布后立刻生效。

9.12.1 修订程序

在CPS中所列条款不能适应运营的实际需求，或者与现行法

律相抵触时，群盾CA有权在合适的时间修订本CPS中任何术语、条件和条款，而且无须预先通知任何一方。

本CPS的修订，由群盾CA安全策略管理委员会组织修订，经安全策略管理委员会审查通过后正式实施。

9.12.2 通知机制和期限

本CPS在群盾CA的网站（http://www.trondun.com）上发布。

版本更新时，最新版本的CPS在群盾CA的网站（http://www.trondun.com）上发布，对具体参与方不做另行通知。

9.12.3 必须修改业务规则的情形

当管辖法律、适用标准及操作规范等有重大改变时，必须修改《电子认证业务规则》。

9.13. 争议处理

如果各参与方之间无法协商解决出现的问题和争端，可通过法律途径解决。对于任何因本CPS有关或由本CPS引起的争议，由群盾CA所在地有管辖权的法院管辖。

9.14. 管辖法律

本规则在各方面服从《中华人民共和国电子签名法》、《电子认证服务管理办法》等中华人民共和国法律、规则、规章、法

令和政令的约束和解释。群盾CA的任何业务活动受有关法律、法规的制约，任何业务和法律文件、合同的解释、执行不能与有关法律、法规相冲突。

9.15. 与适用法律的符合性

本CPS的使用也必须遵从使用地的相关法律和法规。

9.16. 一般条款

9.16.1 完整规定

本《电子认证业务规则》将替代先前的、与主题相关的书面或口头解释。

9.16.2 转让

群盾CA、注册机构、订户及依赖方之间的责任、义务不能通过任何形式转让给其他方。

9.16.3 分割性

法律允许的范围内，在群盾CA订户协议、依赖方协议和其他订户协议内出现可以同其他条款分割的条款时，协议中的可分割条款的无效不应该影响协议中其他条款效力。

9.16.4 强制执行

在群盾CA、注册机构、订户和依赖方之间出现纠纷、诉讼时，

胜讼方可以要求对方支付有关诉讼费作为对其补偿的一部分。免除一方对某次合同违约的赔偿，不意味着免除对其他合同违约的赔偿。

9.16.5 不可抗力

当由于不可抗力，如地震、洪灾、雷电等自然灾害和战争等，造成群盾CA、注册机构无法提供正常的服务时，群盾CA、注册机构不承担由此给客户造成的损失。

9.17. 其他条款

群盾CA对本CPS具有最终解释权。

北京群盾科技有限公司

2023年2月6日