电子认证业务规则规范（试行）

一、电子认证业务规则的主要组成部分

电子认证业务规则是电子认证服务机构对所提供的认证及相关业务的全面描述。电子认证业务规则包括责任范围、作业操作规范和信息安全保障措施等内容，主要由以下几部分组成。

（一）概括性描述

（二）信息发布与信息管理

（三）身份标识与鉴别

（四）证书生命周期操作要求

（五）认证机构设施、管理和操作控制

（六）认证系统技术安全控制

（七）证书、证书吊销列表和在线证书状态协议

（八）认证机构审计和其他评估

（九）法律责任和其他业务条款

二、主要组成部分的内容说明

（一）概括性描述

对电子认证业务规则进行概要性表述，给出文档的名称和标识，指出电子认证活动的参与者及证书应用范围，并说明对电子认证业务规则的管理，最后给出电子认证业务规则中使用的定义和缩写。

1、概述

对电子认证业务规则提供一个概要性介绍，也可用于对电子认证服务机构的概要性描述。例如，可以设定所提供证书的不同保证等级，也可以用图形的方式来表达电子认证服务机构的结构。

2、文档名称与标识

关于电子认证业务规则的任何适用名称或标识符，包括 ASN.1 对象标识符的说明。

3、电子认证活动参与者

* 电子认证服务机构，也就是证书认证机构，是颁发证书的实体。

* 注册机构，也就是为最终证书申请者建立注册过程的实体，对证书申请者进行身份标识和鉴别，发起或传递证书吊销请求，代表电子认证服务机构批准更新证书或更新密钥的申请。

* 订户，从电子认证服务机构接收证书的实体。在电子签名应用中，订户即为电子签名人。

* 依赖方，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。

* 其他参与者，如证书制造机构、证书库服务提供者、以及其他提供电子认证相关服务的实体。

4、证书应用

* 所颁发证书适用的证书应用列表或者类型，如电子邮件、零售交易、合同、旅游订单等。

* 所颁发证书禁止的证书应用列表或者类型。

5、策略管理

描述负责起草、注册、维护和更新当前电子认证业务规则的组织名称和邮件地址，联系人姓名、电子邮件地址、电话号码和传真号码。作为一种替代方案，可不指定真实人，而是定义一个称谓或角色、一个电子邮件别名或其他通用的联系信息。主管部分也可能会制定专门的证书策略，并可指定某个电子认证服务机构的电子认证业务规则符合某种证书策略。如果这样，则需要在此声明批准电子认证业务规则的人或机构，包括名称、电子邮件、电话、传真以及其他常用信息，并说明批准流程。

6、定义和缩写

文档中所使用术语的定义一览表，还包括缩略语及其含义的一览表。例如：

电子认证服务机构（CA）

注册机构（RA）

证书策略（CP）

电子认证业务规则（CPS）

证书吊销列表（CRL）

在线证书状态协议（OCSP）

电子签名认证证书（证书）

电子签名人（证书持有者、订户）

电子签名依赖方（证书使用者、依赖方）

私钥（电子签名制作数据）

公钥（电子签名验证数据）

（二）信息发布与信息管理

描述任何与认证信息发布相关的内容，包括信息库的运营者、运营者的职责、信息发布的频率以及对所发布信息的访问控制等。

1、运营信息库的实体标识，如电子认证服务机构、或独立信息库服务提供者。

2、运营者发布其业务实践、证书和证书当前状态的职责，标识出对公众可用和不可用的项、子项和元素。

3、信息发布的时间和频率。

4、对发布信息的访问控制，包括 CP、CPS、证书、OCSP 和 CRL。

（三） 身份标识与鉴别

描述电子认证服务机构在颁发证书之前，对证书申请者的身份和其他属性进行鉴别的过程，以及标识和鉴别密钥更新请求者和吊销请求者的方法。说明命名规则，包括在某些名称中对商标权的承认问题。

1、命名

* 分配给实体的名称类型，如 X.500 甄别名、RFC-822 名称、X.400 名称。
* 名称是否一定要有意义。
* 订户是否能够使用匿名或假名，如果可以，订户可以使用或将被分配给什么样的名称。
* 理解不同名称形式的规则，如 X.500 标准和 RFC-822。
* 名称是否需要唯一。
* 对商标的承认、鉴别。

2、初始身份确认

* 对机构申请者的组织身份进行身份标识和鉴别的要求，如咨询提供组织身份识别服务的数据库、或检查组织的资质文件。
* 对于个人订户或代表组织订户的个人进行身份标识和鉴别的要求。
* 在初始注册中没有验证的订户信息列表。
* 对机构的验证涉及确定一个人是否具有特定的权力或许可，包括代表组织获取证书的许可。

3、密钥更新请求中的标识与鉴别

针对于密钥更新中对每个实体身份标识和鉴别过程，说明下列元素。

* 常规密钥更新中对身份标识和鉴别的要求，如使用当前有效密钥对包含新密钥的密钥更新请求进行签名。
* 证书被吊销后密钥更新中对身份标识和鉴别的要求，如使用原始身份验证相同的流程。

4、吊销请求中的标识与鉴别

描述对每个实体类型（电子认证服务机构、注册机构、订户或其他参与者）吊销请求的身份标识和鉴别过程。

（四）证书生命周期操作要求

说明在证书生命周期方面对电子认证服务机构及相关实体的要求，注册机构、订户或其他参与者的要求，在每个子项中可能需要对电子认证服务机构、注册机构、订户或其他参与者予以分别考虑。

1、证书申请

* 提交证书申请的实体，如证书申请者或注册机构。

* 实体在提交证书申请时所使用的注册过程，以及在此过程中各方的责任。为了接收证书申请，电子认证服务机构或注册机构可能负有建立注册过程的责任。同样，证书申请者可能负有在其证书申请中提供准确信息的责任。

2、证书申请处理

描述处理证书申请的过程。例如，为了验证证书申请，电子认证服务机构或注册机构可能要执行身份标识和鉴别流程，根据这些步骤，电子认证服务机构 或注册机构将可能依照某些准则或者批准或者拒绝该证书申请。最后，要设置电子认证服务机构或注册机构必须受理并处理证书申请的时间期限。

3、证书签发

* 在证书签发过程中电子认证服务机构的行为，如电子认证服务机构验证注册机构签名和确认注册机构的权限、并生成证书的过程。

* 电子认证服务机构签发证书时对订户的通告机制，如电子认证服务机构用电子邮件将证书发送给订户或注册机构，或者用电子邮件将允许订户到网站下载证书的信息告知用户。

4、证书接受

* 构成申请者接受证书的行为。这种行为可以包括表示接受的确认步骤、暗示接受的操作、没能成功反对证书或其内容。

* 电子认证服务机构对证书的发布方式，例如电子认证服务机构可以将证书发布到 X.500 或 LDAP 证书库。

* 电子认证服务机构在颁发证书时对其他实体的通告，例如，电子认证服务机构可能发送证书到注册机构。

5、密钥对和证书的使用

描述与密钥对和证书使用相关的责任。

* 与订户使用其私钥和证书相关的订户责任。例如，订户可能被要求只能在恰当的应用范围内使用私钥和证书，这些应用在 CP 中设置，并且与有关的证书内容相一致（如密钥用途字段）。

* 与使用订户公钥和证书相关的依赖方责任。例如，依赖方只能在恰当的应用范围内依赖于证书，这些应用在 CP 中设置，并且与有关的证书内容相一致（如密钥用途扩展）。

6、证书更新

证书更新指在不改变证书中订户的公钥或其他任何信息的情况下，为订户签发一张新证书。

* 进行证书更新的情形，如证书已到期，但策略允许继续使用相同的密钥对。

* 请求更新的实体，如订户、注册机构或电子认证服务机构可以自动更新订户证书。

* 为签发新证书，电子认证服务机构或注册机构处理更新请求的过程，如使用令牌，比如口令，来重新鉴别订户、或使用与原始签发证书相同的过程。
* 颁发新证书给订户时的通告。
* 构成接受更新证书的行为。
* 电子认证服务机构对更新证书的发布。
* 电子认证服务机构在颁发证书时对其他实体的通告。

7、证书密钥更新

证书密钥更新指订户或其他参与者生成一对新密钥并申请为新公钥签发一个新证书。

* 证书密钥更新的情形，如因私钥泄漏而吊销证书之后、或者证书到期并且密钥对的使用期也到期之后。
* 可以请求证书密钥更新的实体，如订户。
* 为签发新证书，电子认证服务机构或注册机构处理密钥更新请求的过程。
* 颁发新证书给订户时的通告。
* 构成接受密钥更新证书的行为。
* 电子认证服务机构对密钥更新证书的发布。
* 电子认证服务机构在颁发证书时对其他实体的通告。

8、证书变更

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。

* 证书变更的情形，如名称改变等而造成的实体身份改变。
* 可以请求证书变更的实体，如订户或注册机构。
* 为签发新证书，电子认证服务机构或注册机构处理证书变更请求的过程，如采用与原始证书签发相同的过程。
* 颁发新证书给订户时的通告。
* 构成接受变更证书的行为。
* 电子认证服务机构对变更证书的发布。
* 电子认证服务机构在颁发证书时对其他实体的通告。

9、证书吊销和挂起

* 证书挂起的情形和证书必须吊销的情形，例如订户合同期满、密码令牌丢失或怀疑私钥泄漏。
* 可以请求吊销证书的实体，例如对最终用户证书而言，可能是订户、注册机构或电子认证服务机构。
* 证书吊销请求的流程，如由注册机构签署的消息、由订户签署的消息或由注册机构电话通知。
* 订户可用的宽限期，订户必须在此时间内提出吊销请求。
* 电子认证服务机构必须处理吊销请求的时间。

* 为检查其所依赖证书的状态，依赖方可以或必须使用的检查机制。
* 如果使用 CRL，其发布频率是多少。
* 如果使用 CRL，产生 CRL 并将其发布到证书库的最大延迟是多少（也就是在生成 CRL 之后，在将其发布到证书库中所用的处理和通信相关最长延迟）。
* 在线证书状态查询的可用性，例如 OCSP 和状态查询的 Web 网站。
* 依赖方执行在线吊销状态查询的要求。
* 吊销信息的其他可用发布形式。
* 当因为私钥损害而造成证书吊销或挂起时，上述规定的不同之处（与其他原因造成吊销或挂起相比）。
* 证书挂起的情形。
* 可以请求证书挂起的实体，例如对于最终用户证书而言，订户、订户的上级、或者注册机构。
* 请求证书挂起的过程，如由订户或注册机构签署的消息、或由注册机构电话请求。
* 证书挂起的最长时间。

10、证书状态服务

* 证书状态查询服务的操作特点。
* 查询服务的可用性，以及服务不可用时的适用策略。
* 查询服务的其他可选特征。

11、停止使用认证服务

说明订户停止使用电子认证服务时所使用的过程。

* 停止使用认证服务时的证书吊销（依赖于停止使用认证服务是因为证书到期，还是因为服务终止，可能会有所不同）。

12、密钥生成、备份和恢复

说明与私钥生成、备份和恢复相关的策略和业务实践（通过电子认证服务机构或其他可信第三方）。

* 包含私钥生成、备份和恢复的策略和实践的文档标识，或此类策略和实践一览表。
* 包含会话密钥封装和恢复的策略和实践的文档标识，或此类策略和实践一览表。

（五）认证机构设施、管理和操作控制

描述物理环境、操作过程和人员的安全控制。电子认证服务机构使用这些控制手段来安全地实现密钥生成、实体鉴别、证书签发、证书吊销、审计和归档等功能。也可定义信息库、注册机构、订户或其他参与者的非技术安全控制。

1、物理控制

* 场所区域和建筑，如对高安全区的建筑要求，使用带锁的房间、屏蔽室、保险柜、橱柜。

* 物理访问，也就是从场所的一个区域到另一个区域或进入安全区的访问控制机制。
* 电力和空调。
* 水患防治。
* 火灾预防和保护。
* 介质存储，例如需要在不同的场所利用备份介质进行存储，该场所在物理上是安全的，能够防止水灾和火灾的破坏。
* 废物处理。
* 异地备份。

2、操作过程控制

描述定义可信角色的要求，以及各个角色的责任。可信角色包括系统管理员、安全官员和系统审计员等。声明完成该项任务所需的每个角色人员数，定义对每个角色的身份标识和鉴别要求。按照角色而定义的责任分离，这些角色不能由相同的人承担。

3、人员控制

* 对于充当可信角色或其他重要角色的人员，其需要具备的资格、经历和无过失要求，例如对这些职位的候选者所需具备的信任证明、工作经历和官方凭证。
* 在招聘充当可信角色或其他重要角色的人员时所需背景审查程序，这些角色可能要求调查其犯罪记录、档案。
* 招聘人员后对每个角色的培训要求和过程。
* 在完成原始培训后对每个角色的再培训周期和过程。
* 在不同角色间的工作轮换周期和顺序
* 对下列行为的处罚。未授权行为、未授予的权力使用和对系统的未授权使用等。
* 对独立签约者而非实体内部人员的控制。
* 在原始培训、再培训和其他过程中提供给员工的文档。

4、审计日志程序

描述事件日志和审计系统，实现该系统的目的在于维护一个安全的环境。
* 记录事件的类型，如证书生命周期操作、对系统的访问企图和对系统的请求。
* 处理或归档日志的周期，如每星期、在报警或异常事件之后，或审计日志已满时。
* 审计日志的保存期。
* 审计日志保护。
* 审计日志备份程序。
* 审计日志收集系统是在实体的内部还是外部。
* 是否对导致事件的实体进行通告。
* 脆弱性评估，如审计数据的运行工具破坏系统安全性的潜在可能性估计。

5、记录归档

描述通用的记录归档（或记录保留）策略。

* 归档记录的类型，例如所有审计数据、证书申请信息、支持证书申请的文档。
* 档案的保存期。
* 档案的保护。
* 档案备份程序。
* 对记录加盖时间戳的要求。
* 档案收集系统是内部还是外部。
* 获得和验证档案信息的程序，如由两个人分别来保留归档数据的两个拷贝，并且为了确保档案信息的准确，需要对这两个拷贝进行比较。

6、电子认证服务机构密钥更替

描述电子认证服务机构产生新密钥，并将新的公钥提供给电子认证服务机构用户的过程。此过程可以与产生当前密钥的过程相同，而且可以用旧密钥为新密钥签发证书。

7、损害和灾难恢复

描述与密钥损害或灾难事件相关的通告和恢复过程要求。

* 适用事件和损害的列表，以及对事件的报告和处理过程。
* 对计算资源、软件和（或）数据被破坏或怀疑被破坏的恢复过程，此过程包括如何重建一个安全环境，哪些证书要吊销，实体的密钥是否被吊销，如何将新的实体公钥提供给用户，以及如何为实体重新发证。
* 对实体私钥泄漏的恢复过程，此过程包括如何重建一个安全环境，如何将新的实体公钥提供给用户，以及如何为实体重新发证。
* 自然或其他灾难后实体的业务连续性能力，此能力包括远程热备站点对运营的恢复，也可以包括在灾难发生后到重建安全环境前，或者在原始站点，或者在远程站点保护其设备的程序。

8、电子认证服务机构或注册机构终止

描述与电子认证服务机构或注册机构终止和终止通告相关的过程的要求，包括电子认证服务机构或注册机构档案记录管理者的身份问题。

（六）认证系统技术安全控制

阐述电子认证服务机构为保护其密钥和激活数据（如 PIN 码、口令字或手持密钥共享）而采取的安全措施。

说明对证书库、订户和其他参与者进行的限制，以保护他们的私钥、私钥激活数据和关键安全参数。

描述电子认证服务机构使用的其他技术安全控制手段，用以安全地实现密钥生成，用户鉴别，证书注册，证书吊销，审计和归档等功能。技术控制包含

生命周期安全控制（包括软件开发环境安全，可信的软件开发方法论）和操作安全控制。

1、密钥对的生成和安装

* 生成公、私钥对的实体。可能会是订户、注册机构或电子认证服务机构。密钥对的生成实现方式。

* 私钥安全的提供给实体的方式。可能的方法包括实体自己生成因而自动拥有、用物理的方式将私钥传递给实体、邮寄保存私钥的令牌、或是通过 SSL 会话传递。

* 实体公钥安全地提供给证书认证服务机构的方式。可能通过在线 SSL 会话或经注册机构签署的消息。

* 将电子认证服务机构公钥安全地提供给潜在的依赖方的方式。可能的方式包括用人工将公钥发送给依赖方、用物理方式邮寄一份拷贝给依赖方、或通过 SSL 会话传递。

* 密钥长度。如 RSA 的模长是 1024 比特、DSA 的大素数是 1024 比特。

* 生成公钥参数的实体。生成密钥时是否对参数的质量进行检查。

* 密钥的使用目的，或者密钥的使用目的限制范围。对于 X.509 证书，这些目的需要映射到第三版证书的密钥用途标志位。

2、私钥保护和密码模块工程控制

* 用来产生密钥的模块标准。是否存在与密码模块相关的其他工程或控制。如密码模块边界的标定、输入/输出、角色和服务、有限状态机、物理安全、软件安全、操作系统安全、算法一致性、电磁兼容性和自检测等。

* 私钥是否由 M 选 N 多人控制。如果是，N 和 M 是多少（两人控制是一个特殊的例子，其中 N＝M＝2）。

* 私钥是否被托管。私钥托管的机构，密钥托管（如明文、密文、分割密钥）形式，托管系统的安全控制。

* 私钥是否备份。私钥备份机构，私钥备份（如明文、密文、分割密钥）形式，备份系统的安全控制。

* 私钥是否归档。私钥归档机构，私钥归档（如明文、密文、分割密钥）形式，归档系统的安全控制。

* 私钥可以被导入或导出密码模块的条件。执行此类操作的实体，导入/导出时私钥的形式（如明文、密文、分割密钥）。

* 私钥保存在模块中的形式（如明文、密文、分割密钥）。

* 激活（使用）私钥的实体。为激活私钥必须执行哪些操作（例如登录、上电、提供 PIN、插入令牌/钥匙、自动等等）。一旦私钥被激活，私钥是活动无限长的时间、只活动一次、还是活动于一个定义的时间段。

* 解除私钥激活状态的实体以及方式。解除私钥激活状态的方式包括退出、切断电源、移开令牌/钥匙，自动冻结或者有效期届满。
* 销毁私钥以及方式。销毁密钥的方式包括交出令牌、销毁令牌或者重写密钥。
* 密码模块在下列方面的内容及性能：边界的标定、输入/输出、角色和服务、有限状态机、物理安全、软件安全、操作系统安全、算法一致性、电磁兼容性和自检测。

3、密钥对管理的其他方面

* 公钥是否归档，归档机构实体以及归档系统的安全控制。
* 颁发给订户的证书的操作期，订户密钥对的使用期或生命期。

4、激活数据

说明激活数据的组成和生命周期。

5、计算机安全控制

描述计算机安全控制，计算机系统的安全级别，评估分析和测试。

6、生命周期安全控制

描述系统开发控制、安全管理控制和生命周期安全等级，系统开发控制包括开发环境安全、开发人员安全、产品维护期的配置管理安全、软件工程实施、软件开发方法论、模块化、层次化、使用容错设计和实现技术（如防御性编程）、以及开发工具安全。

安全管理控制包括执行工具和程序，保证操作系统和网络符合设置的安全标准。

7、网络安全控制

说明与网络安全相关的控制，如防火墙、防病毒、入侵检测等。

8、时间戳

说明与对不同数据使用时间戳相关的要求或业务实践，还可声明时间戳应用是否需要使用可信时间源。

（七）证书、证书吊销列表和在线证书状态协议

说明证书、证书吊销列表和在线证书状态协议的格式，包括描述、版本号和扩展项的使用。

1、证书

* 支持的版本号。
* 证书的扩展项及其关键性。
* 密码算法对象标识符。
* 电子认证服务机构、注册机构和订户所使用的名称形式。
* 名称限制及其形式。
* 证书策略对象标识符。
* 策略约束扩展项的使用。

* 策略限定符的语法和语义。
* 对关键证书策略扩展项的处理规则。

2、证书吊销列表

* CRL 支持的版本号。
* CRL 和 CRL 入口扩展项及其关键性。

3、在线证书状态协议

* OCSP 版本号。
* OCSP 扩展项及其关键性。

（八）认证机构审计和其他评估

说明对电子认证服务机构进行审计或评估相关的内容，包括评估所涵盖的主题、评估频率、评估者的资质、评估者与被评估者的资质、对问题所采取的措施以及结果的公告等。

1、评估所涵盖的主题和（或）评估的方法列表。

2、依照某一 CP 或 CPS，对每个实体进行一致性审计或其他评估的频率，或者是引发评估事件的条件。可能的情况如每年一次的年审，运营前评估，或一个疑似或真实安全泄密后的调查。

3、关于执行审计或其他评估的人员的身份和资质。

4、评估者与被评估实体之间的关系，包括评估者的独立程度。

5、对评估中出现的不足所采取的措施，例如暂停运营直到错误得到改正，吊销被评估实体的证书，变换人员，触发特殊调查或增加后续一致性评估频率，宣布被评估实体的损失等。

6、察看审计结果的权限（如被评估实体、其他参与者、公众），提供评估结果的实体（评估者或被评估实体）。

（九）法律责任和其他业务条款

涵盖了一般性的业务和法律问题。在业务条款中说明不同服务的费用问题，和各参与方为了保证资源维持运营，针对参与方的诉讼和审判提供支付所需承担的财务责任。法律责任条款则与通用的技术协定标题相近，涉及保密、隐私、知识产权、担保及免责等内容。

1、费用

* 证书颁发或更新费用。
* 证书访问费用。
* 吊销或状态信息访问费用。
* 其他服务的费用，如对相关 CP 或 CPS 提供访问服务。
* 退款规定。

2、财务责任

* 电子认证服务机构所负有的责任保险范围声明。
* 电子认证服务机构利用其他资源来支持其运营和对潜在责任进行赔付的声明，可以以认证业务正常运营和处理可能意外事件所需的最少财产级别的方式表达，如组织收支平衡表上的财产、保证书、信用证明、在某种条件下要求赔偿的权力契约。
* 电子认证服务机构对其他参与者提供首方责任险或担保保护的程序的声明。

3、业务信息保密
* 被认为是保密信息的范围。
* 被认为在保密信息范围之外的信息类型。
* 接收到保密信息的参与者防止其泄漏、避免使用和发布给第三方的责任。

4、个人隐私保密
* 根据有关法律或政策的需要，指定并公开适用于参与者活动的隐私方案。
* 电子认证活动中认为或者不认为是隐私的信息。
* 接收到隐私信息的参与者保证其安全、避免使用和泄漏给第三方的责任。
* 在使用或者公开其隐私信息时，通知个人或获得个人同意的方面的相应要求。
* 在个人或政府事务或其他任何法律事务中，参与者依据司法或管理程序授权或必须公开隐私信息的条件。

5、知识产权

说明知识产权问题，如版权、专利、商标、商业秘密等。

6、陈述和担保

说明电子认证活动中各种实体所作的陈述和担保。

7、担保免责

对有可能存在其他协议中的明示担保责任的否定描述，对由于适用法律引起的隐含担保责任的描述。在电子认证业务规则中可以直接使用这些担保免责规定，或者包含一项要求，规定担保免责条款要出现在相关协议当中，如订户或依赖方协议。

8、偿付责任限制

说明电子认证业务规则中的偿付责任限制，或者出现在其它相关协议中的偿付责任限制。

9、赔偿

说明一方对另一方遭受损失的赔偿条款，通常这种损失是由第一方的行为所导致的。

10、有效期和终止

包括电子认证业务规则的有效期，以及文档、文档的某一部分或对某一特定参与者的适用性终止的条件。

* 文档的有效期限，也就是文档生效和失效的时间，如果文档不提前终止。
* 终止规定，声明文档、文档的某一部分或对某一特定参与者的适用性停止有效的条件。
* 文档终止的任何可能结果，例如协议的某些条款在协议终止后继续有效，如知识产权承认和保密条款。另外，终止可能涉及到各参与方返还保密信息到其拥有者的责任。

11、对参与者的个别通告与沟通

说明电子认证活动中某一参与方与另一参与方进行通信时可以或必须遵循的方法，以使其通信过程在法律上有效。

12、修订

* 修订电子认证业务规则所应遵循的修订程序。
* 通告机制（将建议的变更通知所有受影响的对象，如订户和依赖方）和周期。
* 需要变更电子认证业务规则的条件。

13、争议处理

说明出自电子认证业务规则的争端的解决程序，例如要求争端需要通过某个机构解决，或者其他的争端解决机制。

14、管辖法律

说明对电子认证业务规则生效和解释起作用的有关法律、法规。

15、与适用法律的符合性

说明电子认证活动参与者所需遵守的适用法律，如与密码硬件和软件相关的法律，该法律可能还受控于给定司法管辖域下的出口控制法。

16、一般条款

* 完整协议条款，通常标识出构成这个协议的全部文档，并声明该协议替代所有先前或同时期的、与相同主题相关的书面或口头解释。
* 转让条款，在该协议下将一方的权利转让给另一方或授权其某种义务。
* 分割性条款，当法庭或其他仲裁机构判定协议中的某一条款由于某种原因无效或不具执行力时，不会出现因为某一条款的无效导致整个协议无效。
* 强制执行条款，可以声明在合同纠纷中有利的一方有权将代理费作为偿还要求的一部分，或者声明免除一方对合同某一项的违反应该承担的责任，但不意味着继续免除或未来免除这一方对合同其他项的违反应该承担的责任。
* 不可抗力条款，通常用于出现超出受影响方控制的事件的发生时，免除一方或多方对合同的执行责任。通常，免除执行的时间与事件所造成的延迟时间相当。此条款也可包括协议终止的环境和条件。构成不可抗力的事件包括战争、恐怖袭击、罢工、自然灾害、供应商或卖方执行失败、因特网或其他基础设施的瘫痪。不可抗力条 款的起草应与框架的其他部分相一致，并达到适用的服务级别协议。

例如，业务连续性和灾难恢复的责任和能力可以将某些事件置于组织的可控范围之内，如在停电时启用备份电源的义务。

17、其他条款

包括未在上述说明的其他相关内容条款。

三、 电子认证业务规则的标题结构参考模版

电子认证服务机构在编写电子认证业务规则时，可以参考如下标题结构列表。

1. 概括性描述

1.1 概述

1.2 文档名称与标识

1.3 电子认证活动参与者

1.3.1 电子认证服务机构

1.3.2 注册机构

1.3.3 订户

1.3.4 依赖方

1.3.5 其他参与者

1.4 证书应用

1.4.1 适合的证书应用

1.4.2 限制的证书应用

1.5 策略管理

1.5.1 策略文档管理机构

1.5.2 联系人

1.5.3 决定 CPS 符合策略的机构

1.5.4 CPS 批准程序

1.6 定义和缩写

2. 信息发布与信息管理

2.1 认证信息的发布

2.2 发布的时间或频率

2.3 信息库访问控制

3. 身份标识与鉴别

3.1 命名

3.1.1 名称类型

3.1.2 对名称意义化的要求

3.1.3 订户的匿名或伪名

3.1.4 理解不同名称形式的规则

3.1.5 名称的唯一性