北京数字认证股份有限公司
事件型证书策略（CP2）

1.0.1 版

发布日期：2017 年 11 月 9 日

生效日期：2017 年 11 月 9 日

北京数字认证股份有限公司

版本控制表

版本	状态	修订说明	审核/批准人	生效时间
1.0.1	版本发布	新版本发布	公司 CPS 策略管理委员会	2017 年 11 月 9 日

声明

本 CP 全部或者部分支持下列标准：

RFC3647：互联网 X.509 公钥基础设施-证书策略和证书业务声明框架

GB/T 26855-2011：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

目　录

1. 引言

1.1. 概述

北京数字认证股份有限公司（Beijing Certificate Authority Co.,Ltd.，以下简称数字认证公司）于 2001 年 2 月开始运营，是权威、公正的电子认证服务机构。数字认证公司严格按照《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，提供数字证书申请、颁发、存档、查询、废止等服务，并通过以 PKI 技术、数字证书应用技术为核心的产品和服务，为电子活动提供可信身份、可信时间和可信行为的网络信任环境。

事件型数字证书是面向即时业务或者特定业务场景，数字认证公司所设计的一类基于事件型证书专利技术的特殊数字证书。事件型数字证书一般用于一次性事件型数字签名，签名过后私钥销毁，保证各签名参与主体的身份真实性、信息的完整性以及签名行为的不可抵赖性。

证书策略（Certification Policy，以下简称 CP）是关于电子认证服务机构制订的一组规则，表明证书对特定群体的适用范围，或对不同安全需求类型的适用规则。

本《北京数字认证股份有限公司事件型证书策略》（以下简称《事件型证书策略》）满足互联网标准组织制定的 RFC3647《互联网 X.509 公钥基础设施-证书策略和证书业务声明框架》，以及国内标准 GB/T 26855-2011《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》的框架和内容要求。本《事件型证书策略》适用范围为数字认证公司发放的事件型证书。具体设定了证书策略、生命周期、使用、依赖和管理的角色、责任与要求，以及各相关主体的职责。为批准、签发、管理和使用证书和相关的可信服务制定业务，提供技术、策略和法律上的要求和规范。

1.2. 文档名称与标识

本文档的名称为《北京数字认证股份有限公司事件型证书策略（CP2）》，简称《事件型证书策略》，本证书策略 CP 的对象标识符为：1.2.156.112562.2.2.2。

1.3. PKI 参与者

1.3.1. 电子认证服务机构

数字认证公司是根据《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（简称：CA 机构）。

CA 机构是受用户信任，负责创建和分配公钥证书的权威机构，是颁发数字证书的实体。

1.3.2. 注册机构

注册机构作为电子认证服务机构授权委托的下属机构，包括注册系统（简称：RA 系统）和证书本地受理点，负责受理证书申请。

1.3.3. 订户

订户是从 CA 机构接收数字证书的实体。在电子签名应用中，订户即为电子签名人。

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。在本业务中，是信任数字认证公司签发的事件型证书，可以对使用事件型证书机制进行的数字签名验证的实体。

1.3.5. 其他参与者

其他参与者指为 CA 证书服务体系提供相关服务的其他实体。

1.4. 证书应用

1.4.1. 适合的证书应用

本 CA 机构签发的事件型证书适合应用在企业信息化、电子政务和电子商务等领域，用于证明订户在电子化环境中所进行的电子签名行为。

1.4.2. 限制的证书应用

本 CA 机构发放的数字证书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负责。

1.5. 策略管理

1.5.1. 策略文档管理机构

本《事件型证书策略》的管理机构是数字认证公司 CPS 策略管理委员会。由数字认证公司 CPS 策略管理委员会负责本《事件型证书策略》的制订、发布、更新等事宜。

1.5.2. 联系人

本《事件型证书策略》在数字认证公司网站发布，对具体个人不另行通知。

网站地址：http://www.bjca.cn

电子邮箱地址：cps@bjca.org.cn

联系地址：北京市海淀区北四环西路 68 号双桥大厦 15 层(左岸工社)(100080)

电话号码：8610-58045600

传真号码：8610-58045678

1.5.3. 决定 CP 符合策略的机构

本《事件型证书策略》由数字认证公司 CPS 策略管理委员会组织制定，报数字认证公司 CPS 策略管理委员会批准实行。

1.5.4. CP 批准程序

本《事件型证书策略》由数字认证公司 CPS 策略管理委员会审批通过后，在数字认证公司的网站上对外公布。

本《事件型证书策略》经数字认证公司 CPS 策略管理委员会审批通过后，从对外公布之日起三十日之内向工业和信息化部备案。

1.6. 定义和缩写

下列定义适用于本《事件型证书策略》：

a) 公开密钥基础设施（PKI）Public Key Infrastructure

支持公开密钥体制的安全基础设施，提供身份鉴别、加密、完整性和不可否认性服务。

b) 证书策略（CP）Certification Policy

是关于电子认证服务机构制订的一组规则，表明证书对特定群体的适用范围，或对不同安全需求类型的适用规则。

c) 电子认证业务规则(CPS) Certification Practice Statement

关于证书电子认证服务机构在签发、管理、吊销或更新证书(或更新证书中的密钥)过程中所采纳的业务实践的声明。

d) 电子认证服务机构（CA）Certification Authority

受用户信任，负责创建和分配公钥证书的权威机构。

e) 注册机构 Registration Authority

具有下列一项或多项功能的实体：识别和鉴别证书申请人，同意或拒绝证书申请，在某些环境下主动撤销或挂起证书，处理订户撤销或挂起其证书的请求，同意或拒绝订户更新其证书或密钥的请求。但是，RA 并不签发证书（即 RA 代表 CA 承担某些任务）。

f) 事件型数字证书：AnySign Certificate

事件型数字证书是面向即时业务或者特定业务场景，数字认证公司所设计的一类基于事件型证书专利技术的特殊数字证书。在业务过程中，自动将业务场景中相关信息（电子文档、签名行为特征信息、手写笔迹或其他签名行为证据信息等）关联至数字证书的扩展域，签发出事件型数字证书，实现业务过程中的可靠电子签名。事件型数字证书所对应的私钥一般为一次性使用，其在使用一次后即被销毁。

在本 CP 中，如无特殊定义，所述的数字证书，均指事件型数字证书。

g) 私钥(电子签名制作数据) Private Key

指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。

私钥是经由数字运算产生的密钥，用于制作电子签名数据，亦可依据其运算方式，就相对应的公开密钥加密的文件或信息予以解密。

h) 公钥(电子签名验证数据) Public Key

公钥是经由数字运算产生的密钥，用于解密电子签名，确认电子签名人的身份及电子签名的真实性。

公钥可以公开，一般标示于在线数据库、存储库或其他公共目录中，使任何希望得到公钥的人都能得到。

电子签名验证数据是指用于验证电子签名的数据，包括代码、口令、算法或者公钥等。如果电子签名制作数据表现为私钥，则电子签名验证数据就是公钥。

2. 信息发布与信息管理

2.1. 信息库

本 CA 机构的信息库是一个对外公开的信息库，面向订户及依赖方提供信息服务。提供信息服务包括但不限于以下内容：CPS 和 CP 以及数字认证公司不定期发布的信息。

2.2. 认证信息的发布

本《事件型证书策略》发布在数字认证公司的网站上，供相关方下载、查阅。

2.3. 发布时间或频率

本《事件型证书策略》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。

2.4. 信息库访问控制

对于公开发布的 CP 和 CPS 等公开信息，数字认证公司允许公众自行通过网站进行查询和访问。

3. 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（Distinguished Name，简称 DN）。

数字证书中的主体的 X.500 DN 是 C=CN 命名空间下的 X.500 目录唯一名字。

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 CA 证书服务体系中，订户(证书申请人)不宜使用匿名或伪名。

3.1.4. 理解不同名称形式的规则

数字证书符合 X.509 标准，甄别名格式遵守 X.500 标准。甄别名的命名规则由数字认证公司定义。

3.1.5. 名称的唯一性

在 CA 认证服务体系中，不同订户的证书主体的名称是唯一的。但对于同一订户，可以用其主体名为其签发多张证书，但证书的扩展项不同。

3.1.6. 商标的承认、鉴别和角色

CA 机构签发的证书不包含任何商标或者可能对其他机构构成侵权的信息。

3.2. 初始身份确认

3.2.1. 证明持有私钥的方法

事件型证书申请人在签名行为发生时，产生证书请求包括申请人的身份信息，以及证书申请人在进行签名行为时的记录信息（包括证书申请人的签名场景、签名动作、签名内容对象或签名内容特征值，从而可以事后有效还原签名行为）。签名行为的记录信息与证书申请人的身份信息在证书申请时进行绑定。因此，在签名行为发生时证书申请人视作其私钥的唯一持有者。

3.2.2. 订户身份的鉴别

事件型证书订户身份的鉴别参照个人身份鉴别方法，订户在为电子签名行为申请事件型证书前，应通过个人身份鉴别，有效证明订户身份，接受事件型证书申请的有关条款，同意承担相应的责任。

在事件型证书鉴别过程中，由 CA 机构或授权的注册机构，接受订户的证书申请，对订户的身份真实性进行审核，并采集和记录订户的身份信息和电子签名行为的记录信息。

3.2.3. 没有验证的订户信息

订户提交鉴证文件以外的信息为没有验证的订户信息。

3.2.4. 授权确认

当申请者代表委托人申请证书时，需要出示足够的证明信息以证明个人是否真实存在，申请者是否已获得委托人的授权。CA 机构和授权的注册机构有责任确认该授权信息，并将授权信息妥善保存。

3.2.5. 互操作准则

互操作可能是交叉认证、单身交叉认证或其他形式的互操作。交叉认证是指两个完全独立的、采用各自认证策略的 CA 中心之间建立相互信任关系，从而使双方的订户可以实现互相认证。

CA 机构将根据业务需要，在遵循本《事件型证书策略》的各项控制要求的基础上，与 CA 的证书服务体系中未涉及的其他电子认证服务机构建立交叉认证

关系。但交叉认证并不表示本 CA 机构批准了或赋予了其他 CA 中心或电子认证服务机构的权力。

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

事件型证书的密钥只适用于一次性签名事件，没有证书密钥更新服务。

3.3.2. 吊销后密钥更新的标识与鉴别

事件型证书的密钥只适用于一次性签名事件，不涉及吊销后密钥更新服务。

3.3.3. 证书变更的标识与鉴别

事件型证书的密钥只适用于一次性签名事件，没有证书变更服务。

3.4. 吊销请求的标识与鉴别

事件型证书只针对即时性签名事件，证书使用后即时失效，没有证书吊销服务。

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

证书申请实体仅包括个人订户。

4.1.2. 申请过程与责任

证书申请人按照《事件型证书策略》和《电子认证服务规则》所规定的要求，准备相关的身份证明材料提交至 CA 机构或授权的注册机构，CA 机构或授权的注册机构依据身份鉴别规范对证书申请人的身份进行鉴别，并决定是否受理申请。

申请过程中各方责任为：

订户：订户需要提供 3.2 所述的有效身份证明材料，并确保材料真实准确，配合 CA 机构或授权的注册机构完成对身份信息的采集、记录和审核。

CA 机构：CA 机构参照 3.2 的要求对订户的身份信息进行采集、记录，审核。通过鉴证后，CA 机构向订户签发证书。如果用户身份信息的鉴别由授权的注册机构完成，CA 机构应对授权的注册机构进行监督管理和审计。

根据《中华人民共和国电子签名法》的规定，证书申请者未向 CA 机构提供真实、完整和准确的信息，或者有其他过错，给 CA 机构或电子签名依赖方造成损失的，应承担相应的法律责任和经济赔偿。

4.2. 证书申请处理

4.2.1. 执行识别与鉴别功能

证书申请者向 CA 机构或授权的注册机构提交初始的证书申请请求，注册机构须按照以下规定对订户的申领材料进行审查，参照 3.2.2 节的规定。

4.2.2. 证书申请批准和拒绝

CA 机构或授权的注册机构根据本《事件型证书策略》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。

证书申请人通过身份鉴别流程且鉴证结果为合格，CA 机构或授权的注册机构将批准证书申请，CA 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，CA 机构或授权的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

事件型证书申请为即时处理。

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

CA 机构在批准证书申请之后，将签发证书。证书的签发意味着电子认证服务机构最终完全正式地批准了证书申请。

4.3.2. 电子认证服务机构对订户的通告

事件型证书用于标识和证明订户的电子签名行为，CA 机构为订户签发证书后，将直接应用于对应的电子签名。订户成功完成电子签名，即视为 CA 机构证书签发成功，CA 机构不再就证书签发向订户进行其他方式的通告。

4.4. 证书接受

4.4.1. 构成接受证书的行为

事件型证书签发完成后，并将证书应用于对应的电子签名时起，就被视为同意接受证书。

4.4.2. 电子认证服务机构对证书的发布

根据依赖方要求提供证书发布。

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 CA 签发事件型证书，CA 机构不对其他实体进行通告。

4.5. 密钥对和证书的使用

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 CA 机构所签发的证书后，均视为已经同意遵守与 CA 机构和依赖方有关的权利和义务的条款。

事件型证书仅应用于订户对应的电子签名行为，订户只能在该次电子签名中使用私钥和证书，订户只有在接受了相关证书之后，才能使用对应的私钥执行电子签名运算。私钥将在完成本次电子签名数学运算后进行销毁，之后订户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）。依赖方获得对方的证书和公钥后，可以通过查看对方的证书了解对方的身份，并通过公钥验证对方电子签名的真实性。

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

事件型证书仅用于订户特定一次的电子签名行为，没有证书更新服务。

4.7. 证书密钥更新

事件型证书密钥在使用过一次后即销毁，没有证书密钥更新服务。

4.8. 证书变更

事件型证书仅用于订户特定一次的电子签名行为，没有证书变更服务。

4.9. 证书吊销和挂起

事件型证书仅用于订户特定一次的电子签名行为，密钥在使用过一次后即销毁，没有证书吊销和挂起服务。

4.10. 证书状态服务

事件型证书仅用于订户特定一次的电子签名行为，证书使用一次后即失效，根据依赖方约定，可向依赖方提供状态查询服务。

4.11. 订购结束

事件型证书订购结束是指当订户使用数字证书完成电子签名后，该证书的服务时间结束。

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

订户的签名密钥对由签名设备生成密钥并执行签名后，即时销毁，签名密钥不进行保管。

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

本章规定参见 CPS。

6. 认证系统技术安全控制

6.1. 密钥对的生成和安装

6.1.1. 密钥对的生成

CA 系统和 RA 系统的密钥对是在加密机内部产生，加密机具有国家密码主管部门的相应资质。在生成 CA 密钥对时，CA 机构按照加密机密钥管理制度，执行详细的操作流程控制计划，选定并授权 3 个密钥管理员，密钥管理员凭借智能 IC 卡对密钥进行控制。

事件型证书订户的签名密钥由签名设备生成。

6.1.2. 私钥传送给订户

订户的签名密钥对由签名密码设备生成并保管。

6.1.3. 公钥传送给证书签发机构

订户的签名证书公钥通过安全通道，经注册机构传递到 CA 机构。

从 RA 到 CA 以及从密钥管理中心到 CA 的传递过程中，采用国家密码主管部门许可的通讯协议及密钥算法，保证了传输中数据的安全。

6.1.4. 电子认证服务机构公钥传送给依赖方

依赖方可以从数字认证公司的网站(http://www.bjca.cn)下载根证书和 CA 证书，从而得到 CA 的公钥。

6.1.5. 密钥的长度

密钥算法和长度符合国家密码主管部门规定。

6.1.6. 公钥参数的生成和质量检查

公钥参数由国家密码主管部门许可的加密设备生成。对生成的公钥参数的质量检查标准，这些设备内置的协议、算法等均符合国家密码主管部门要求。

6.1.7. 密钥使用目的

订户的签名密钥可以用于提供安全服务，实现身份认证、不可抵赖性和信息的完整性等，用于签署具备法律效力的电子文档和电子交易数据。

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

CA 机构所用的密码设备都是经国家相关部门认可的产品，其接口、协议、密钥和物理安全要符合国家相关规范要求。

6.2.2. 私钥的多人控制

CA 证书的私钥的生成、更新、吊销、备份和恢复等操作采用多人控制机制，即采取三选二方式，将私钥的管理权限分散到 3 张管理员卡中，只有其中半数以上管理员在场并许可的情况下，才能对私钥进行上述操作。

6.2.3. 私钥托管

无。

6.2.4. 私钥备份

CA 私钥备份在专用密码设备中。

6.2.5. 私钥归档

通过数据库备份出来进行归档保存。

6.2.6.私钥导入或导出密码模块

使用 CA 软件可以把私钥安全导入到密码模块中，CA 私钥无法从硬件密码模块中导出。

6.2.7.私钥在密码模块中的存储

CA 私钥在硬件密码模块中加密保存。

6.2.8.激活私钥的方法

具有激活私钥权限的管理员使用含有自己的身份的加密 IC 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

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加密 IC 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场。

6.2.10.销毁密钥的方法

具有销毁密钥权限的管理员使用含有自己的身份的加密 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

CA 机构使用具有国家密码主管部门颁发商用密码型号证书的服务器密码机，符合国家有关标准。

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，由 CA 机构定期归档。

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和其对应的密钥对的有效期都是一致的。

6.4. 激活数据

无。

6.5. 计算机安全控制

6.5.1. 特别的计算机安全技术要求

为了保证系统的正常运行，对所需要的计算机设备进行正确的选型、验收，制定操作规范。另外，本系统采用增加冗余资源的方法，使系统在有故障时仍能正常工作。

6.5.2. 计算机安全要求

CA 系统建设符合《GB22239-2008 信息系统安全等级保护基本要求》的第三级要求。

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

CA 机构对系统的维护保证操作系统、网络设置和系统配置安全。通过日志检查来检查系统和数据完整性和硬件的正常操作。

6.6.3. 生命周期的安全控制

整个系统从设计到实现，系统的安全性始终是重点保证的。完全依据国家有关标准进行严格设计，使用的算法和密码设备均通过了主管部门鉴定，使用了基于标准的强化安全通信协议确保了通信数据的安全，在系统安全运行方面，充分考虑了人员权限、系统备份、密钥恢复等安全运行措施，整个系统安全可靠。

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。CA 机构采取防火墙、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

时间戳系统提供的时间戳服务在技术实现上严格遵循国际标准时间戳协议（RFC3161），采用标准的时间戳请求、时间戳应答以及时间戳编码格式，时间源采用国家授时中心提供的标准时间。

7. 证书格式

7.1. 证书

CA 签发的证书符合 X.509 V3 格式。遵循 RFC3280 标准。

7.1.1. 版本号

X.509 V3。

7.1.2. 算法对象标识符

符合国家密码主管部门批准的算法对象标识符。

7.1.3. 名称形式

CA 数字证书中的主体 Subject 的 X.500 DN 是 C=CN 命名空间下的 X.500 目录唯一名字，各属性的编码一律使用 UTF8String。

主体 Subject 的 X.500 DN 支持多级 O 和 OU，其格式如下：

C=CN;

O=××

OU= ××;

CN=××

- C（Country）应为 CN，表示中国；
- O（Organization）应为证书主体或者证书主体所属单位的所在省、自治区、直辖市名称全称。可选部分；
- OU（Organization Unit）应为证书主体或者证书主体所属单位的名称全称。可选部分；
- CN（Common Name）应为证书主体的姓名；

7.1.4. 证书扩展项

CA 证书扩展项除使用 IETF RFC 3280 中定义的证书扩展项，还支持私有扩展项。

CA 采用的 IETF RFC 3280 中定义的证书扩展项：

- 颁发机构密钥标识符 Authority Key Identifier

- 使用者密钥标识符 Subject Key Identifier
- 密钥用法 Key Usage

私有扩展项可支持以下类型：

- 签名证据项：Signature Evidences，应包含签名相关证据内容，如声音、图像等。

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

审计是为了检查、确认 CA 是否按照《事件型证书策略》和《电子认证业务规则》及其理制度和安全策略开展业务，发现存在的可能风险。根据工作需要，定期组织开展审计评估。

8.2. 评估者的资质

内部审计人员由 CA 机构内部人员组成，外部审计的审计人员的资质由第三方确定。

8.3. 评估者与被评估者之间的关系

评估者与被评估者应无任何业务、财务往来或其它利害关系，足以影响评估的客观性。

8.4. 评估内容

审计所涵盖的主题包括：人事、机房物理安全、安全运营管理、密钥安全和运行服务、客户服务等内容。

8.5. 对问题与不足采取的措施

对审计中发现的问题，CA 机构将根据审计报告的内容准备解决方案，明确对此采取的行动。CA 机构将根据国际惯例和相关法律、法规迅速解决问题。

8.6. 评估结果的传达与发布

除非法律明确要求，CA 机构一般不公开评估结果。

对 CA 关联方，CA 机构将依据签署的协议来公布评估结果。

9. 法律责任和其他业务条款

本章规定参见 CPS。