腾讯云 CA

CA 证书法律合规说明

腾讯云

【版权声明】

【商标声明】

【服务声明】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或95716。

文档目录

CA 证书法律合规说明
证书使用须知

最近更新时间：2024-07-12 09:07:41

腾讯云 CA 的产品设计严格遵循《中华人民共和国民法典》、《电子认证服务管理办法》、《中华人民共和国电子签名法》的各项规定，具备充分的法律效力。同时在使用前您还需要关注以下内容：

证书批量管理风险须知

在您使用证书批量管理功能前，请务必仔细阅读以下注意事项：

1. 证书批量管理仅支持批量管理证书更新、证书吊销，暂不支持其他证书管理批量操作，如有其他需求可使用单个证书管理功能。
2. 证书批量管理涉及到两个及以上证书信息变更，将会影响证书所属者使用，批量操作前，请您务必保证证书更新及/或吊销已通知被管理的证书所属者并获得其同意，且您申请批量管理的证书信息需确保准确、真实、完整。
3. 证书批量管理会涉及用量消耗，由此产生的费用由管理证书所在机构承担。
4. 证书批量管理须由管理证书所在机构认证时授权的经办人本人操作，否则由此造成的所有风险及法律责任由管理证书所在机构自行承担。
5. 您与被管理的证书所属者之间因证书管理产生的纠纷，与腾讯云CA及数字证书服务机构无关，由您与被管理的证书所属者自行解决，如因此造成腾讯云CA及/或数字证书服务机构损失的，您需一并赔偿。
6. 您承诺使用证书批量管理功能不存在违反相关法律法规、腾讯云CA产品相关协议及规则的规定，亦不存在侵犯第三方合法权益的情形，且不会利用该功能从事违法违规活动。
7. 请您谨慎使用证书批量管理功能，如因错误操作导致证书不可用、被吊销等情况，由您自行承担。

单个证书管理用户须知（总）

在您使用证书管理功能前，请务必仔细阅读以下注意事项：

1. 证书管理功能包括证书更新、证书信息变更、证书补办、证书冻结、证书解锁、证书吊销等功能，您可根据具体需求使用相关功能。
2. 如您是企业用户，证书管理功能可由管理证书所在机构认证时授权的经办人本人操作，亦可由您授权的经办人自行操作；如您是个人用户，证书管理功能由证书所属者本人操作。否则由此产生的所有风险及法律责任，均由您自行承担。
3. 证书管理涉及到证书信息变更，将会影响证书使用。您使用证书管理功能前，请仔细复核所提交的相关信息，如因错误操作导致证书不可用、被吊销等情况，由您自行承担。
4. 证书管理会涉及用量消耗及费用支付，您需要和管理证书所在机构就用量、费用等事项协商一致，如因此产生费用纠纷，均与腾讯云CA及数字证书服务机构无关，由您负责解决，如因此造成腾讯云CA及/或数字证书服务机构损失的，您需一并赔偿。
5. 您承诺使用证书管理功能不存在违反相关法律法规、腾讯云CA产品相关协议及规则的规定，亦不存在侵犯第三方合法权益的情形，且不会利用该功能从事违法违规活动。

证书更新用户须知

在您使用证书更新功能前，请务必仔细阅读以下注意事项：

1. 如您是企业用户，证书更新功能可由管理证书所在机构认证时授权的经办人本人操作，亦可由您授权的经办人自行操作；如您是个人用户，证书更新功能由证书所属者本人操作。否则由此产生的所有风险及法律责任，均由您自行承担。
2. 证书有效期为一年，证书到期后需要续费更新，才能正常使用。
3. 您可在证书有效期届满前90天至届满后30天内[腾讯法务1] 申请在线更新证书，超过前述申请期限的，您无法使用证书更新功能，仅可重新申请证书。
4. 如您在申请期限内在线申请更新的，则新证书有效期在旧证书截止日期的基础上顺延一年。
5. 证书在线更新后，证书密码不变。
6. 证书更新涉及到证书信息变更，将会影响证书使用。您使用证书更新功能前，请仔细复核所提交的相关信息，如因错误操作导致证书不可用、被吊销等情况，由您自行承担。
7. 证书更新需消耗管理证书所在机构的证书用量。在线申请普通证书更新前，您需要和管理证书所在机构就用量、费用等事项协商一致，如因此产生费用纠纷，均与腾讯云CA及数字证书服务机构无关，由您与管理证书所在机构自行解决，如因此造成腾讯云CA及/或数字证书服务机构损失的，您需一并赔偿。
8. 您承诺使用证书更新功能不存在违反相关法律法规、腾讯云CA产品相关协议及规则的规定，亦不存在侵犯第三方合法权益的情形，且不会利用该功能从事违法违规活动。

证书信息变更用户须知

在您使用证书信息变更功能前，请务必仔细阅读以下注意事项：

1. 如您是企业用户，证书信息变更功能可由管理证书所在机构认证时授权的经办人本人操作，亦可由您授权的经办人自行操作；如您是个人用户，证书信息变更功能由证书所属者本人操作。否则由此产生的所有风险及法律责任，均由您自行承担。
2. 证书有效期内发生信息变更的（如企业名称变更等），您应及时在线提交信息变更申请。因您未及时申请证书信息变更导致的证书使用风险及法律后果由您自行承担，且因此导致腾讯云CA及/或数字证书服务机构损失的，您需一并赔偿。
3. 您使用证书信息变更功能前，请仔细复核所提交的相关信息，如因错误操作导致证书不可用、被吊销等情况，由您自行承担。
4. 重新签发的证书有效期与原证书一致。
5. 证书信息变更需消耗管理证书所在机构的证书用量。在线申请普通证书信息变更前，您需要和管理证书所在机构就用量、费用等事项协商一致，如因此产生纠纷，均与腾讯云CA及数字证书服务机构无关，由您与管理证书所在机构自行负责解决，如因此造成腾讯云CA及/或数字证书服务机构损失的，您需一并赔偿。
6. 您承诺使用证书更新功能不存在违反相关法律法规、腾讯云CA产品相关协议及规则的规定，亦不存在侵犯第三方合法权益的情形，且不会利用该功能从事违法违规活动。

证书补办用户须知

在您使用证书补办功能前，请务必仔细阅读以下注意事项：

1. 如您不慎将证书介质USBkey丢失或者需要更换证书所在服务器，请您及时申请证书丢失补办。请您知悉，因证书介质USBkey丢失、未及时进行证书补办申请等情形所导致的证书使用风险及法律后果由您自行承担，且因此导致腾讯云CA及/或数字证书服务机构损失的，您需一并赔偿。
2. 如您是企业用户，证书补办功能可由管理证书所在机构认证时授权的经办人本人操作，亦可由您授权的经办人自行操作；如您是个人用户，证书补办功能由证书所属者本人操作。否则由此产生的所有风险及法律责任，均由您自行承担。
3. 您使用证书信息补办功能前，请仔细复核所提交的相关信息，如因错误操作导致证书补办失败、证书不可用等情况，由您自行承担。证书成功补办后，原证书将被吊销，证书有效期与原证书一致。
4. 在线申请普通证书补办前，您需要和管理证书所在机构就用量、费用等事项协商一致，其中，证书补办需消耗管理证书所在机构的证书用量，如还涉及补办ukey的，则可能额外产生ukey购买费用及邮费等费用。如因此产生费用相关纠纷，均与腾讯云CA及数字证书服务机构无关，由您与管理证书所在机构自行负责解决，如因此造成腾讯云CA及/或数字证书服务机构损失的，您需一并赔偿。
5. 您承诺使用证书补办功能不存在违反相关法律法规、腾讯云CA产品相关协议及规则的规定，亦不存在侵犯第三方合法权益的情形，且不会利用该功能从事违法违规活动。

证书解锁用户须知

在您使用证书解锁功能前，请务必仔细阅读以下注意事项：

1. 如您是企业用户，证书解锁功能可由管理证书所在机构认证时授权的经办人本人操作，亦可由您授权的经办人自行操作；如您是个人用户，证书解锁功能由证书所属者本人操作。否则由此产生的所有风险及法律责任，均由您自行承担。
2. 如果您的证书ukey已被锁定，我们提供2种解决方式，请任意选择其中一种：
   2.1 请将ukey邮寄给以下地址并留存您接收解锁后ukey的收件人手机和地址。我们将在收到Ukey且复核您的身份后，将尽快为您解锁并按照您指定地址邮寄返还，其中往来的快递费用都将由您本人承担 。

   地址：内蒙古自治区呼和浩特市赛罕区锡林郭勒南路恩和大厦9号楼1508-9
   邮政编码：010010
   收件人：高先生
   官方咨询电话：0471-5610214

   2.2 请使用证书补办功能并更换新ukey。
3. 在线申请普通证书解锁前，需要和管理证书所在机构就用量、费用等事项协商一致。其中，证书解锁需消耗管理证书所在机构的证书用量，如还涉及补办ukey的，则可能额外产生ukey购买费用及邮费等费用。如因此产生费用相关纠纷，均与腾讯云CA及数字证书服务机构无关，由您与管理证书所在机构自行负责解决，如因此造成腾讯云CA及/或数字证书服务机构损失的，您需一并赔偿。
4. 您承诺使用证书解锁功能不存在违反相关法律法规、腾讯云CA产品相关协议及规则的规定，亦不存在侵犯第三方合法权益的情形，且不会利用该功能从事违法违规活动。

证书吊销用户须知

在您使用证书吊销功能前，请务必仔细阅读以下注意事项：

1. 如您需停止使用数字证书，您可申请证书吊销。请您知悉，证书吊销后则不能继续使用，如因错误操作导致证书不可用、被吊销等情况，由您自行承担。
2. 如您是企业用户，证书吊销功能可由管理证书所在机构认证时授权的经办人本人操作，亦可由您授权的经办人自行操作；如您是个人用户，证书吊销功能由证书所属者本人操作。否则由此产生的所有风险及法律责任，均由您自行承担。
3. 吊销后如需使用证书服务须重新申请证书。
4. 证书吊销需消耗管理证书所在机构的证书用量。在线申请普通证书吊销前，需要和管理证书所在机构就用量、费用等事项协商一致。如因此产生费用相关纠纷，均与腾讯云CA及数字证书服务机构无关，由您与管理证书所在机构自行负责解决，如因此造成腾讯云CA及/或数字证书服务机构损失的，您需一并赔偿。
5. 您承诺使用证书吊销功能不存在违反相关法律法规、腾讯云CA产品相关协议及规则的规定，亦不存在侵犯第三方合法权益的情形，且不会利用该功能从事违法违规活动。

证书冻结用户须知

1. 如您发现证书可能出现信息泄露等情形时，您可申请证书冻结。请您知悉，如因您未及时申请证书冻结所导致的证书使用风险及法律后果由您自行承担，且因此导致腾讯云CA及/或数字证书服务机构损失的，您需一并赔偿。
2. 如您是企业用户，证书吊销功能可由管理证书所在机构认证时授权的经办人本人操作，亦可由您授权的经办人自行操作；如您是个人用户，证书吊销功能由证书所属者本人操作。否则由此产生的所有风险及法律责任，均由您自行承担。
3. 证书冻结期间，您无法使用证书服务，请您谨慎操作。如因错误操作导致证书不可用等情况，由您自行承担。
4. 证书冻结后，如需进行证书更新、证书吊销等操作，须先进行证书解冻申请。
5. 证书冻结需消耗管理证书所在机构的证书用量。在线申请普通证书冻结前，需要和管理证书所在机构就用量、费用等事项协商一致，如因此产生费用相关纠纷，均与腾讯云CA及数字证书服务机构无关，由您与管理证书所在机构自行负责解决，如因此造成腾讯云CA及/或数字证书服务机构损失的，您需一并赔偿。
6. 您承诺使用证书冻结功能不存在违反相关法律法规、腾讯云CA产品相关协议及规则的规定，亦不存在侵犯第三方合法权益的情形，且不会利用该功能从事违法违规活动。

数字证书使用许可授权须知

最近更新时间：2024-09-04 15:54:11

普通数字证书用户（企业/自然人）在腾讯云官网申请、使用、管理其名下普通企业/个人证书资源之前，需要先取得管理证书所在企业/机构授权同意。管理证书所在企业/机构下发《腾讯云 CA 数字证书使用许可授权书》，即意味着管理证书所在企业/机构知晓并同意：

- 管理证书所在企业/机构同意某某企业/自然人申请、使用、管理其名下的普通企业/个人证书资源。
- 管理证书所在企业/机构知晓某某企业/自然人申请、使用、管理其名下的普通企业/个人证书涉及到的法律责任及义务，并承担相应风险。
- 普通证书用户管理过程中，涉及到其管理证书所在机构的经办人短信/邮件授权，会及时配合。

授权书下载

- 腾讯云 CA 数字证书使用许可授权书

腾讯云 CA 验签须知

最近更新时间：2024-09-04 15:54:11

1. 本验证意见书是针对使用数字证书等电子签名签署的电子数据的验证结果。
2. 申请人在申请数字证书电子签名验证前需确保数字证书有效，验证机构不对无效数字证书出具验证意见。
3. 申请人应当提供真实、完整、准确的验证材料，并对验证材料的真实性、合法性负责。
4. 验证机构依照法律、法规和规章规定的方式、方法和步骤，遵守和采用相关技术标准和技术规范进行验证。
5. 验证机构依法独立、客观、公正地进行验证，不受任何组织和个人的非法干预。
6. 使用本验证意见书应当保持其完整性和合法性。
7. 未经电子数据信息权属人同意，申请人不得将本验证意见书用于违背权属人意愿之用途，且不得用于非法用途。
8. 验证机构不对没有通过本机构完成的实名认证、意愿认证和其他签署过程承担任何证明或担保责任。
9. 术语和定义。
   9.1 电子签名，是指数据电文中以电子形式所含、所附用于识别签名人身份并表明签名人认可其中内容的数据。通俗的说，电子签名就是通过密码技术对电子数据的电子形式的签名，并非是书面签名的数字图像化，而是类似于手写签名或盖章，通过电子签名可以验证签名人的身份以及签名人是否认可电子数据的内容。
   9.2 数字签名，是指基于PKI/CA技术，通过使用数字证书以及非对称密码加密技术与数字摘要技术对电子数据进行加密及签名的一种电子签名。采用数字签名的电子数据，可以通过签名验签等技术方式客观识别认证发件人（即签名人）的身份并验证电子数据的完整性，因此，数字签名具有抗抵赖性（即不可否认性）。

特别说明，电子签名验证信息中“证书使用者”字段的“值”完整内容包括 CN、O、OU、E 等，一般情况下，CN 项载明数字证书的“证书所有者”；O 项载明证书所在机构的机构名；OU 项用来表示证书的类型和用来表示证书发放机构的标识；E 项载明 e-mail 地址或不用。

腾讯云 CA 法律效力说明

最近更新时间：2024-09-04 15:54:11

法律条款对照说明

2005年颁布、2019年修订的《中华人民共和国电子签名法》确立了电子签名的法律效力：

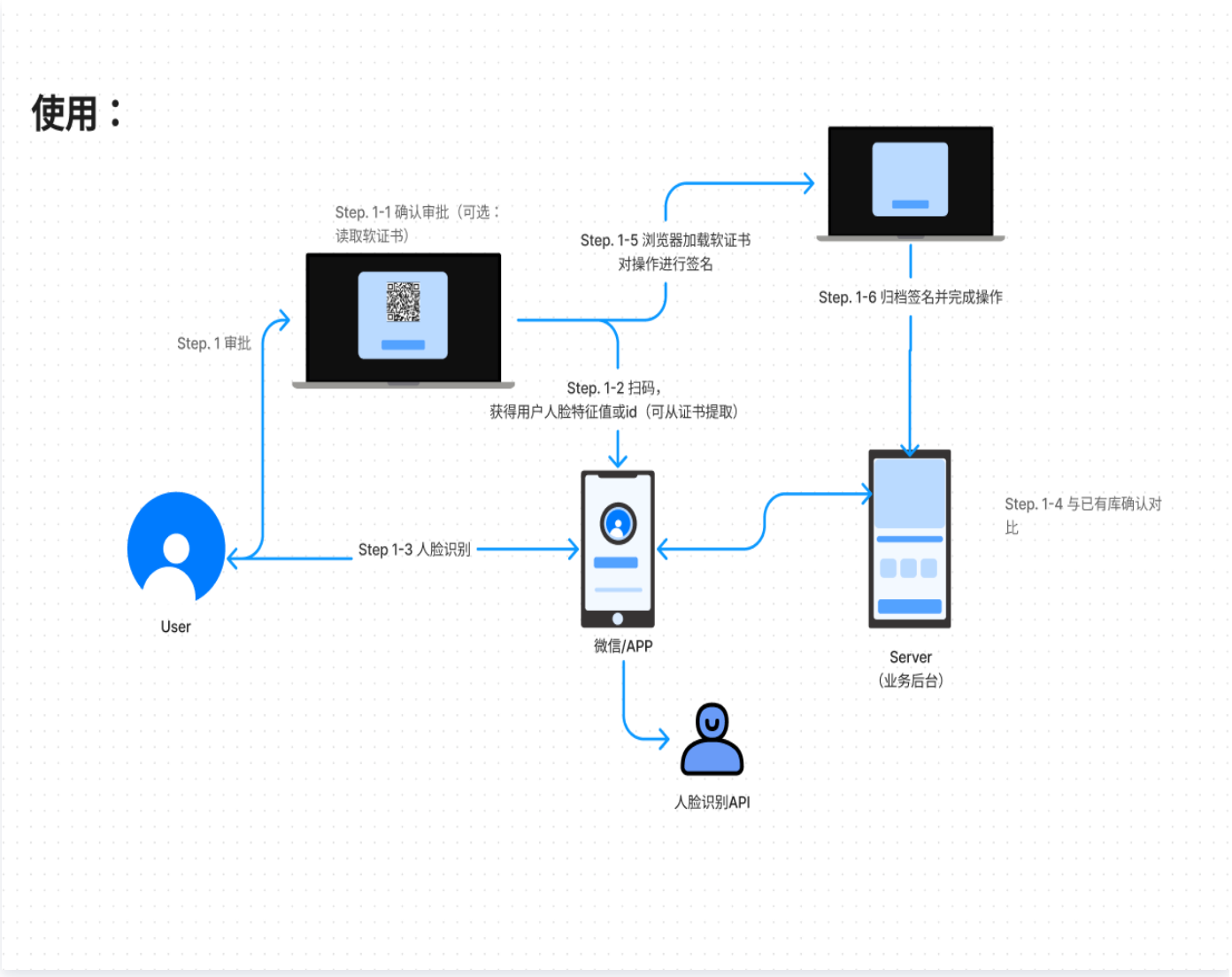
- 《电子签名法》第三条规定“当事人约定使用电子签名、数据电文的文书，不得仅因为其采用电子签名、数据电文的形式而否定其法律效力”。
- 《电子签名法》第十三条规定了视为可靠电子签名的条件。
- 《电子签名法》第十四条规定“可靠的电子签名与手写签名或者盖章具有同等法律效力”。
- 《电子签名法》第十六条规定“电子签名需要第三方认证的，由依法设立的电子认证服务提供者提供认证服务”。

腾讯云 CA 作为具备**电子认证服务许可证、电子认证服务使用密码许可证**的权威、公正的第三方电子认证机构，具有认证机构采用的电子缔约技术符合中国法律及其相关法规，根据国家市场准入政策由国家主管部门批准，具有权威性；采用的密码算法及技术保障是高度安全的，是具有可信任性；是不参与交易双方利益的第三方机构，在《电子签名法》中被称作"电子认证服务提供者"，其形成的数据电文或电子缔约文件符合中国法律规定，与纸质文件具有同样的法律效力。腾讯云 CA《数字证书服务协议》《腾讯云 CA 数字证书服务合同》与《中华人民共和国电子签名法》内容对照详情请见：

长效证书（个人、企业），时间戳的使用及效用

通过数字证书，我们在以计算机为基础的电子化事务处理中或者敏感数据处理时采用电子化签名的形式，即电子签名或称为数字签名，常见的可以有长效证书（个人、企业）签名、数字时间戳标记，也可以同时使用获得更全面保障：

1. 长效证书（个人、企业长效证书）的数字签名，用于辨别数据签署人的身份，并表明签署人对数据信息的认可，使得数据信息具有易验证性和不可抵赖性的双重特性。



长效证书持有者在审批操作确认时，使用其个人长效证书进行数字签名，携带该数字签名的审批事务信息具有易验证性和不可抵赖性的双重特性，可以在客户端和服务端进行证据留存。结合腾讯云 CA 机构出具的对于审批者个人长效证书的证书验证报告，形成有效的证据组合。

2. 数字时间戳提供了一种对可信时间标记的服务，经数字签名获得的时间戳数据可以用来证明在某一时刻数据发生或存在，并进一步支持数据的抗抵赖。对于电子商务应用，经常要求参与交易各方不能否认某一时刻的交易行为， 但由于用户桌面时间很容易改变，所以应当在调用权威第三方时间戳服务数字签名并形成可信赖的时间戳数据，从而解决一系列的实际和法律问题。

在审批操作确认时，除了第1部分里的个人长效证书数字签名外，需进一步将携带该数字签名的审批事务信息发送到第三方权威（CA）时间戳数字签名服务，进一步形成可信赖的时间戳数据。

验证报告及样例

在客户通过安全工具使用数字证书对交易信息进行加密和签名的条件下，腾讯云 CA 将保证交易信息的保密性、完整性、抗抵赖性。如果发生纠纷，将依据不同情形承担下述义务：

1. 提供签发客户数字证书的 CA 证书。

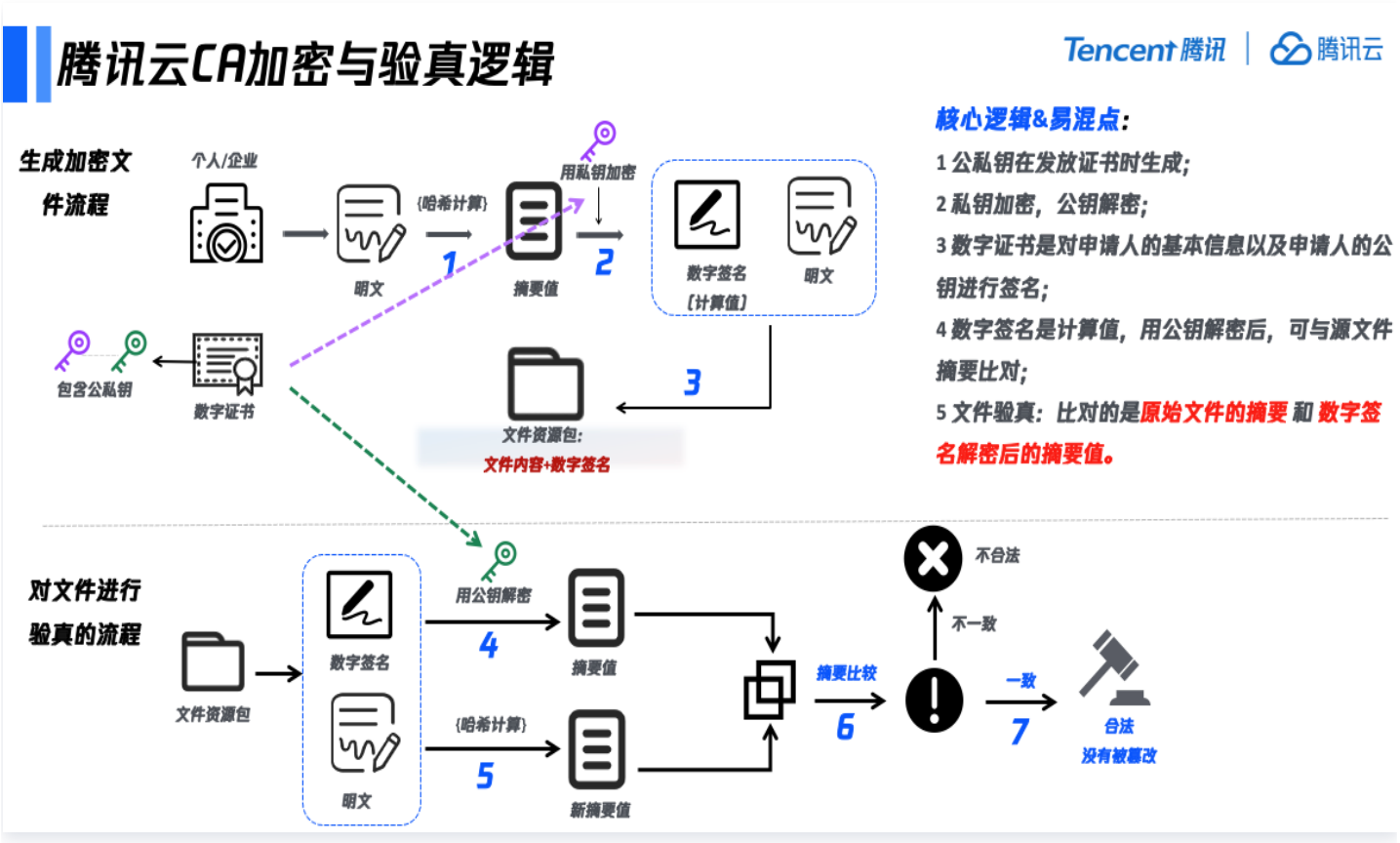
2. 提供客户数字证书在交易发生时，是否在腾讯云 CA 发布的数字证书废止列表（即 CRL）的证明。

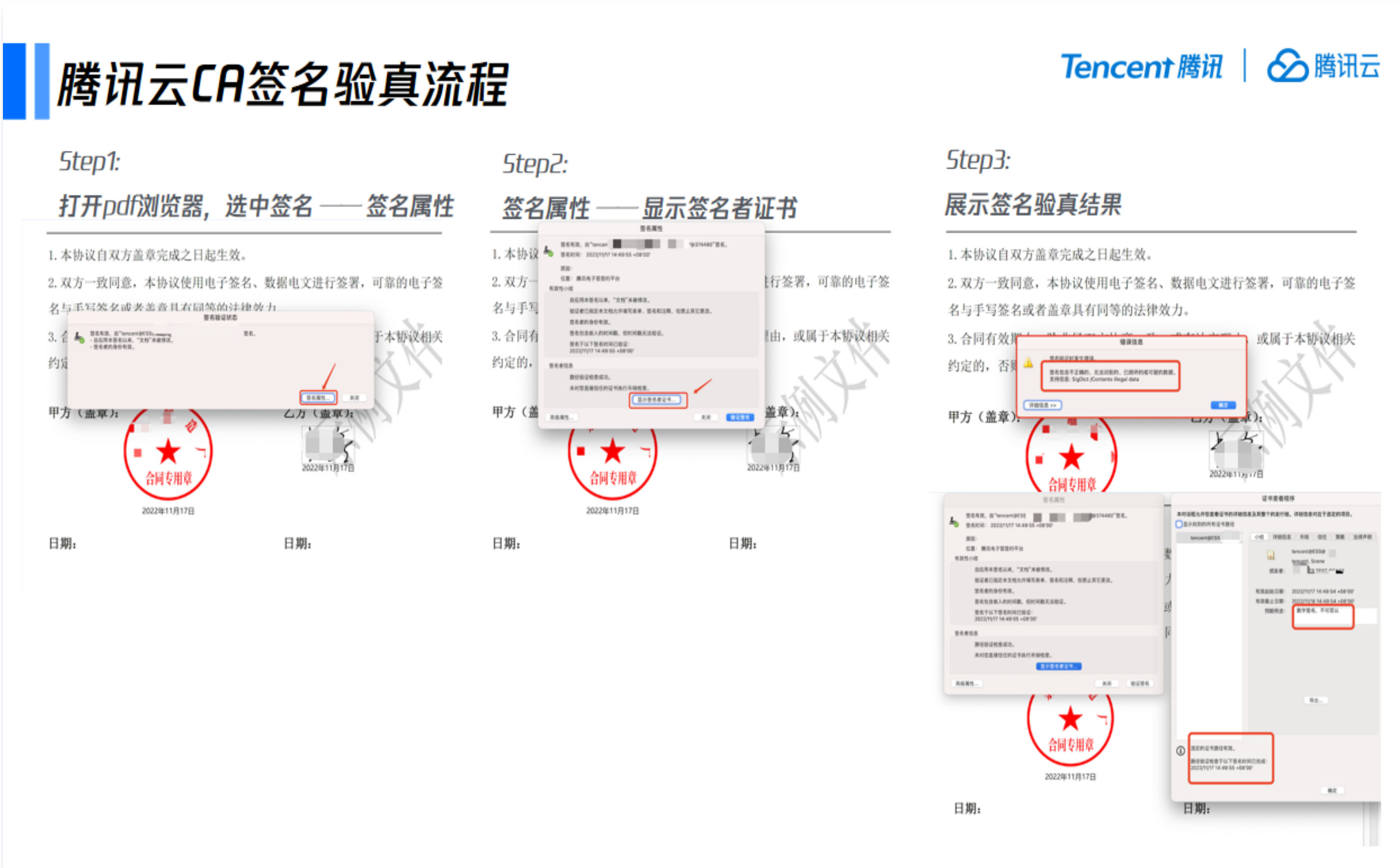
3. 对数字证书、数字签名、时间戳的真实性、完整性进行技术确认，并出具对应的数字或纸质报告（需申请）。

腾讯云 CA 将提供的数字签名验证意见书样例请参见 腾讯云 CA 数字签名验证意见书-模板 。

附录：验真逻辑

除了正式的验证报告，客户可以对于 CA 证书签署过的数据信息自行进行验真，以腾讯云 CA 文件加密与验真逻辑、签名与验真逻辑为例，如下图所示：




腾讯云CA签名验真流程
Tencent腾讯
腾讯云
Step1:
打开pdf浏览器，选中签名 —— 签名属性
Step2:
签名属性 —— 显示签名者证书
Step3:
展示签名验真结果
1. 本协议自双方盖章完成之日起生效。
2. 双方一致同意，本协议使用电子签名、数据电文进行签署，可靠的电子签名与手写签名或者盖章具有同等的法律效力。
甲方（盖章）：
乙方（盖章）：
合同专用章
2022年11月17日
日期：

电子认证服务机构的作用

最近更新时间：2024-12-12 14:50:02

一、相关法律法规

数字证书由电子认证服务机构（CA）颁发，为人员、机构、设备入网提供身份安全、访问控制、数据安全等是网络安全基础能力，广泛应用在公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域。《中华人民共和国密码法》《商用密码管理条例》《中华人民共和国电子签名法》《电子政务移动办公系统安全技术规范》等法律法规，均明确了电子认证服务机构提供服务的必要性。

《电子认证服务管理办法》第五条规定，电子认证服务机构应当具备下列条件：

（一）具有独立的企业法人资格。

（二）具有与提供电子认证服务相适应的人员。从事电子认证服务的专业技术人员、运营管理人员、安全管理人员和客户服务人员不少于三十名，并且应当符合相应岗位技能要求。

（三）注册资本不低于人民币三千万元。

（四）具有固定的经营场所和满足电子认证服务要求的物理环境。

（五）具有符合国家有关安全标准的技术和设备。

（六）具有国家密码管理机构同意使用密码的证明文件。

（七）法律、行政法规规定的其他条件。

《电子认证服务管理办法》第十七条规定，电子认证服务机构应当保证提供下列服务：

（一）制作、签发、管理电子签名认证证书。

（二）确认签发的电子签名认证证书的真实性。

（三）提供电子签名认证证书目录信息查询服务。

（四）提供电子签名认证证书状态信息查询服务。

二、以商用密码为中心的合规观点

2.1《商用密码条例》与《电子签名法》衔接，确立电子认证商用密码管控要求

2023年7月生效的《商用密码条例》在《密码法》的基础上，对电子认证服务机构及电子政务电子认证服务机构应该遵循的要求分别作出了规定，具体对照内容如下：

	电子认证服务机构	电子政务电子认证服务机构
资质要求	依法取得国家密码管理部门同意使用密码的证明文件	依法取得电子政务电子认证服务机构资质
业务规范	应当按照法律、行政法规和电子认证服务密码使用技术规范、规则，使用密码提供电子认证服务，保证其电子认证服务密码使用持续符合要求。	应当按照法律、行政法规和电子政务电子认证服务技术规范、规则，在批准范围内提供电子政务电子认证服务，并定期向主要办事机构所在地省、自治区、直辖

		市密码管理部门报送服务实施情况。
技术关联	《信息安全技术电子政务移动办公系统安全技术规范》“终端基础环境安全通用配置应支持数字证书的安装和运行，采用的密码算法符合国家密码主管部门的规定；**数字证书**应存储在密码产品中，外置存储设备接口受限的移动终端可采用安全薄膜卡或虚拟硬件密码模块等方式。”	

2.2 制度协同，明确电子认证合规必备性

《商用密码条例》规定，对于符合条件的商用密码产品应经过检测认证合格后方可销售、提供。对于列入“网络关键设备和网络安全专用产品目录”的商用密码产品以及使用网络关键设备和网络专用产品的商用密码服务，应该履行网络关键设备和网络专用产品的检测认证合规义务。《商用密码条例》规定，关键信息基础设施运营者如涉及在其所运营的关键信息基础设施上使用商用密码的情况，需承担商用密码应用安全性评估及检测认证的义务：

（1）安全性评估义务：应在关键信息基础设施投入运营前自行或者委托商用密码检测机构开展商用密码应用安全性评估；在投入运营后每年至少进行一次评估，评估情况按照国家有关规定报送国家密码管理部门或者关键信息基础设施所在地省、自治区、直辖市密码管理部门备案。

（2）检测认证合规义务：使用的商用密码产品、服务应当经检测认证合格；使用的密码算法、密码协议、密钥管理机制等商用密码技术应当通过国家密码管理部门审查鉴定。

此外，《网络安全法》第二十三条对上述合规义务做出了规定，《关于修改<中华人民共和国网络安全法>的决定（征求意见稿）》第一条明确了违反《网络安全法》第二十三条的法律责任。如《中华人民共和国网络安全法（修订征求意见稿）》最终生效，则对于提供未经检测认证的网络关键设备和网络专用产品的网络产品提供者而言，应核查自身业务是否涉及《网络关键设备和网络安全专用产品目录》，并对需要落实商用密码检测认证的业务进行合规性整改，使用商用密码保护网络安全，并根据监管要求接入具备资质的电子认证服务机构。

电子签名与《电子签名法》

最近更新时间：2024-09-04 15:54:11

一、电子签名法修订历史

《中华人民共和国电子签名法》2004年8月28日第十届全国人民代表大会常务委员会第十一次会议通过，根据2015年4月24日第十二届全国人民代表大会常务委员会第十四次会议《关于修改〈中华人民共和国电力法〉等六部法律的决定》第一次修正，根据2019年4月23日第十三届全国人民代表大会常务委员会第十次会议《关于修改〈中华人民共和国建筑法〉等八部法律的决定》第二次修正。

二、什么是电子签名?

根据《中华人民共和国电子签名法》相关规定，电子签名，是指数据电文中以电子形式所含、所附用于识别签名人身份并表明签名人认可其中内容的数据。所称数据电文，是指以电子、光学、磁或者类似手段生成、发送、接收或者储存的信息。电子签名同时符合下列条件的，视为可靠的电子签名：
（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。

电子签名相关术语

（一）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。
（二）电子签名依赖方，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人。
（三）电子签名认证证书，是指可证实电子签名人与电子签名制作数据有联系的数据电文或者其他电子记录。
（四）电子签名制作数据，是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。
（五）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。

三、法律认可的数据电文

符合下列条件的数据电文，视为满足法律、法规规定的原件形式要求：
（一）能够有效地表现所载内容并可供随时调取查用。
（二）能够可靠地保证自最终形成时起，内容保持完整、未被更改。但是，在数据电文上增加背书以及数据交换、储存和显示过程中发生的形式变化不影响数据电文的完整性。
符合下列条件的数据电文，视为满足法律、法规规定的文件保存要求：
（一）能够有效地表现所载内容并可供随时调取查用。
（二）数据电文的格式与其生成、发送或者接收时的格式相同，或者格式不相同但是能够准确表现原来生成、发送或者接收的内容。
（三）能够识别数据电文的发件人、收件人以及发送、接收的时间。

四、可信时间戳的重要性

时间对于法律文件（例如合同）而言是极为重要的因素。时间戳（Time stamp）是一种计算机术语，是指电子文件产生的时间。个人计算机产生电子文件后的时间取决于该台计算机设备的时钟，而此类时钟可以任意修改，因此在普通个人计算机设备上形成的电子文件的时间戳因难以证明不可篡改性而没有一般意义上的证据效力。但一个国家的标准时间是具有权威性的，每个国家的标准时间由各国权威授时中心管理。“可信时间戳”就是由可信的第三方时间戳服务中心（TSA）颁发的证明电子文件产生时间的电子凭证。

电子签名法明确了数据电文收发时间定义，数据电文进入发件人控制之外的某个信息系统的时间，视为该数据电文的发送时间。

收件人指定特定系统接收数据电文的，数据电文进入该特定系统的时间，视为该数据电文的接收时间；未指定特定系统的，数据电文进入收件人的任何系统的首次时间，视为该数据电文的接收时间。这里所提到的时间，即需要可信时间戳作为法律认可的电子凭证。

工信部许可的55家 CA 机构

最近更新时间：2024-09-04 15:54:11

中华人民共和国工业和信息化部许可的55家 CA 机构名单如下（来源：工业和信息化部政务服务平台）：

序号	CA 机构名称	地区
1	中金金融认证中心有限公司	北京
2	北京天威诚信电子商务服务有限公司	北京
3	北京数字认证股份有限公司	北京
4	颐信科技有限公司	北京
5	北京国富安电子商务安全认证有限公司	北京
6	联通智慧安全科技有限公司	北京
7	北京中认环宇信息安全技术有限公司	北京
8	中铁信弘远（北京）软件科技有限责任公司	北京
9	北京世纪速码信息科技有限公司	北京
10	农信银资金清算中心有限责任公司	北京
11	中国电力科学研究院有限公司	北京
12	泰尔认证中心有限公司	北京
13	国汽（北京）智能网联汽车研究院有限公司	北京
14	广东省电子商务认证有限公司	广东
15	数安时代科技股份有限公司	广东
16	深圳市电子商务安全证书管理有限公司	广东
17	卓望数码技术（深圳）有限公司	广东
18	沃通电子认证服务有限公司	广东
19	江苏省国信数字科技有限公司	江苏
20	江苏智慧数字认证有限公司	江苏

21	江苏国密数字认证有限公司	江苏
22	南京数字认证有限公司	江苏
23	东方中讯数字证书认证有限公司	重庆
24	重庆程远未来电子商务服务有限公司	重庆
25	大陆云盾电子认证服务有限公司	重庆
26	湖南省数字认证服务中心有限公司	湖南
27	东方新诚信数字认证中心有限公司	湖南
28	苏博云科数字认证有限公司	湖南
29	天津市滨海数字认证有限公司	天津
30	天津市中环认证服务有限公司	天津
31	上海市数字证书认证中心有限公司	上海
32	亚数信息科技（上海）有限公司	上海
33	山东省数字证书认证管理有限公司	山东
34	山东豸信认证服务有限公司（原山东云海）	山东
35	华测电子认证有限责任公司	河南
36	河南省信息化发展有限公司	河南
37	浙江省数字安全证书管理有限公司	浙江
38	云南省数字证书认证中心有限公司	云南
39	新疆数字证书认证中心（有限公司）	新疆
40	四川省数字证书认证管理中心有限公司	四川
41	陕西省数字证书认证中心股份有限公司	陕西
42	山西省数字证书认证中心（有限公司）	山西
43	西部安全认证中心有限责任公司	宁夏
44	内蒙古网信电子认证有限责任公司	内蒙
45	辽宁数字证书认证管理有限公司	辽宁

46	江西省数字证书有限公司	江西
47	吉林省安信电子认证服务有限公司	吉林
48	湖北省数字证书认证管理中心有限公司	湖北
49	黑龙江省数字证书认证有限公司	黑龙江
50	河北省电子认证有限公司	河北
51	海南省信安电子认证有限公司	海南
52	贵州省电子证书有限公司	贵州
53	广西壮族自治区数字证书认证中心有限公司	广西
54	福建省数字安全证书管理有限公司	福建
55	安徽省电子认证管理中心有限责任公司	安徽