

域信(vTrus)数字证书使用协议

版本 1.3

请您在申请、接受或使用任何域信数字证书之前，必须仔细阅读本协议。如果您不同意本协议的条款，请不要申请、接受或使用该证书。若您接受本协议内容，从您申请证书开始，您已同意和接受本协议中所有条款的约束力。如果您对于本协议中相关条款有任何问题，请您发送邮件到 compliance@itrus.com.cn 进行询问。

协议双方为天威诚信和证书申请人或订户，自证书申请之日起生效。

1. 信息准确：用户在任何时候都有义务和保证向天威诚信提供真实、准确和完整的证书申请信息，包括：证书请求文件、身份证明材料等天威诚信要求的与签发证书类型相应的资料；(I)如果在证书申请中所做的陈述变更或不再有效，用户需通知天威诚信；(II)用户提供的证书信息(包括任何电子邮件地址)不侵犯任何第三方的知识产权；(III)用户提供的证书信息(包括任何电子邮件地址)均未且不会用于任何非法目的；

2. 密钥保护：用户在任何时候都有责任和义务采取有力的措施来保证证书密钥的安全，证书密钥必须由专人保管，不得外泄，并保管好密钥密码；用户，或被授权的用户，是唯一一个拥有密钥，管理密码，PIN，软件或硬件机制保护密钥的主体；

3. 证书验收：用户有责任和义务在收到证书后检查和核实证书内容的准确性；一旦用户使用服务器证书，用户应对相关使用行为自行负责，并自行承担因使用行为所产生的一切后果；如果用户在收到服务器证书 24 小时内未明确表示拒绝，就表示接受该证书；

4. 证书使用和限制：用户有责任和义务只在证书主题备用名称中列出的绑定域名的服务器中安装证书，并保证在使用过程中遵守所有适用的法律法规和本使用条款；不应该使用：(I)代表任何其他组织；(II)非证书申请人进行包含相应域名及/或组织名称的证书公私钥的运营；(III)在危险环境中使用需要确保安全性能的设备(如核设施的操作、航空器导航或通信系统、空中交通管制系统、武器控制系统等)时，不能使用。如果用户使用在多个物理服务器设备中，用户默认承认并同意该选项会增加网络的安全风险，并且天威诚信明确否认对跨多个设备的单个密钥分发导致的安全漏洞的任何责任。(IV)服务器证书申请人的申请获得批准，申请人即成为服务器证书用户。申请人保证本人为域名的持有人或经授权的托管人，若采取欺诈等手段获取服务器证书，经查证属实的，天威诚信有权撤销该服务器证书。在服务器证书有效期内因使用该服务器证书给他人造成损失的，由申请人自行承担赔偿责任。

5. 私钥保护：您同意遵守加密硬件安全模块(HSM)上的私钥保护要求。您已知悉以下所示内容并将使用硬件安全模型(HSM)来存储为域信(vTrus)PDF文档签名证书生成的一个或多个私钥(I)您知悉并确认将私钥安全地存储在HSM中，以防止删除；(II)您知悉并确认HSM或者通过审核的云HSM配置都属于您单独控制或使用；(III)您知悉并确认不会在HSM之外使用私钥；(IV)您知悉并确认私钥在满足或超过FIPS 140-2 2级(或同等标准)或通用标准EAL4+的加密模块中才获得有效保护；(V)您同意仅在合适的硬件加密模块中为证书生成密钥对。

6. 证书吊销：用户有责任和义务在以下情况下立刻停止使用证书，并立刻向天威诚信申请吊销证书：(I)证书中信息不正确或不准确，或由于证书申请单位信息变更而变成不正确或不准确，或(II)任何实际或涉嫌被滥用或证书密钥丢失或证书损坏等；(III)用户必须保证服务器证书有效期内域名持有人不得变更，如果域名转让，天威诚信有权吊销服务器证书，并不退还用户已缴纳的费用。新域名持有人若欲继续使用服务器证书，需重新申请新的服务器证书。(IV)服务器证书不得转让、出租或者转借，如果发生转让、出租或者转借，天威诚信有权吊销该服务器证书。因转让、出租或者转借所产生的一切后果由用户承担。

证书吊销原因包含以下几种情况：

- **keyCompromise：**证书私钥泄露；
- **privilegeWithdrawn：**用户在其证书请求中提供了误导性信息，或未履行其在用户协议或使用条款下的重大义务等违规行为但未导致密钥泄露；
- **cessationOfOperation：**拥有证书的网站在证书到期前被关闭，或用户不再拥有或控制证书中的域名；

- **affiliationChanged:** 证书中的主体名称或其他主体身份信息已经更改;
- **superseded:** 证书废止, 用户申请新的证书替代原有的证书, CA机构有合理的证据表明证书中的域名和IP地址的授权无效或CA机构发现证书不符合CP/CPS、BR或者本协议中的任何一个。

7. 证书终止使用: 如果由于证书密钥泄漏而被吊销, 则用户有义务并应保证立即停止使用此证书公钥和密钥;

8. 反馈义务: 用户有义务在指定时间内回应天威诚信关于密钥泄漏或证书被滥用的通知;

9. 信息处理: 如果(I)证书或证书申请者被确定为非法行为;(II)证书申请者身份无法验证和核实;或(III)并非证书申请者提出证书被吊销申请(如:发现密钥被泄露、发现证书签名恶意软件等),则用户同意天威诚信共享证书申请者信息给其他 CA、行业组织和国际 CA/浏览器标准联盟。(IV)基于服务需要,建议您同意授权天威诚信对您提供的个人信息以及个人敏感信息进行处理。您可以选择不向天威诚信提供某些类型的信息,但是这可能会限制您使用部分或全部电子认证服务。当天威诚信通过系统、程序、人工询问等方式向您核实或请求授权处理您的个人信息时,会尽量解释这些限制,以便您做出决定。(V)如部分服务涉及跨境业务,天威诚信需要向境外机构传输境内收集的相关个人信息的,天威诚信会按照法律法规和相关监管部门的规定执行,向您说明个人信息出境的目的以及涉及的个人信息类型,征得您的同意。

10. 周知和接受: 用户必须周知并接受:(I)如证书申请单位/证书申请人违反本使用条款,或天威诚信发现用户的证书被用来从事如钓鱼式攻击、欺诈或传播恶意代码等犯罪活动或其他违反有关法律法规时,天威诚信有权立即吊销该证书。(II)天威诚信承诺在现有技术条件下,由天威诚信签发的服务器证书不会被伪造、篡改。如果服务器证书被篡改,经确认确属天威诚信的责任,由天威诚信承担赔偿责任。承担赔偿责任的范围及方法见《天威诚信全球信任体系认证业务规则(CPS)》。(III)用户同意天威诚信因业务发展需要将本协议项下天威诚信承担的权利与义务转让予第三方。

11. 已阅读和接受 CPS: 用户在注册和申请天威诚信数字证书之前,必须仔细阅读《天威诚信全球信任体系认证业务规则(CPS)》,并同意和接受 CPS 中所有条款。

12. 退款说明: 如果您对该证书不满意,证书生效之日起30天内,请提出申请吊销证书并申请该证书的全额退款。证书生效之日起30天后,不予退款。

13. 法律依据: (I)《天威诚信全球信任体系认证业务规则(CPS)》为本协议的组成部分,与本协议具有同等法律效力,天威诚信有权根据技术情况的变化对该规则做出调整。(II)本协议履行过程中发生争议的,双方同意应优先友好协商解决;协商未果的,可通过法律途径解决。任何一方均可向天威诚信工商注册所在地人民法院提起诉讼,生效判决对双方均具有约束力。(III)本协议适用中华人民共和国法律。