

UniTrust Global 订户协议 ver1.14

本订户协议(“本协议”)由您及您代表的公司、组织或其他实体(“您”)与上海市数字证书认证中心有限公司(“SHECA”, “UniTrust”)之间签订。

申请 UniTrust 证书表示申请人或机构及其经办人同意授权 SHECA 使用证书申请资料用于电子认证业务,并按照相关法律法规及监管要求妥善存储此类资料。申请证书即同意 SHECA 个人信息保护政策,具体请见官方网站:
<https://www.sheca.com>。

本协议自证书申请之日起生效,请仔细阅读本协议。使用 UniTrust 签发的证书,即视为您已充分阅读、理解并同意本订户协议的全部条款与条件。如果您不同意本协议或本协议中的任何条款,那么您应在证书生效之日起的 30 个自然日内取消您的订单并获得全额退款。如果您对本协议有任何问题,您可以联系 policy@sheca.com 获得解答。

一. 定义和术语

AATL: 指 Adobe Approved Trust List, 由 Adobe 公司维护的根证书入根计划。

PDF: 全称为可移植文档格式,是一种用独立于应用程序、硬件、操作系统的方式呈现文档的文件格式。

CA: 指依法设立的第三方电子认证服务机构,是具有公信力的,是根据 CP 和 CPS 的要求签发、撤销和管理证书的实体,就本协议而言,CA 指 UniTrust。

证书申请人: 指向申请证书的自然人或法人实体,证书颁发后,申请人被视为订户。订户:接受证书且遵守订户协议和使用条款的自然人或法人实体。

申请代表人: 也称经办人,是指代表申请人提交证书申请的自然人或个人担保人,必须为申请人本人,或受雇于申请人,或获明确授权代表申请人;申请代表人也可代申请人提交证书撤销申请。

公钥与私钥: 公钥与私钥是通过一种算法得到的一个密钥对(即一个公钥和一个私钥),公钥是密钥对中公开的部分,私钥则是非公开的部分。

证书/数字证书: 指 CA 签发的由数字签名绑定公钥和订户信息的电子文档。

SSL/TLS 证书: 安全套接字层(Secure Socket Layer, SSL)是用来确保 Internet 通信和事务安全的最常见的标准,SSL/TLS 证书就是遵守安全套接字层协议,由受信任的 CA 机构,在进行严格的验证后颁发,具有服务器身份验证和数据传输加密功能。SSL/TLS 证书根据验证级别分为域名型 SSL 证书(简称 DV SSL)、组织型 SSL 证书(简称 OV SSL)和增强型 SSL 证书(简称 EV SSL)三种类型。

通配符证书: 证书中主题备用名称所列的任意域名最左侧包含“*”的 SSL/TLS 证书。

代码签名证书: 通过对代码进行数字签名来标识软件来源以及软件开发者的真实身份并保证代码在签名之后不被恶意篡改的数字证书。

时间戳签名: 确认数据在某一时间(之前)是已经存在的、完整的、可验证的,时间戳签名主要用于数据防篡改和事后抵赖,确定数据产生的准确时间。

证书透明度: 也称证书透明、证书透明化,它是一个实验性的 IETF 开源标准和开源框架,目的是监测和审计数字证书。

密钥泄露: 如果私钥被泄漏给未经授权的人,且未经授权的人可以访问或使用私钥,则称私钥被泄露。

主题备用名称: 是一项对 X.509 的扩展,它允许在 SSL/TLS 证书中使用 subjectAltName 字段将多种值与证书关联,这些值被称为主题备用名称。

CRL: 证书撤销列表是尚未到期就被证书颁发机构撤销的数字证书的名单。这些在证书撤销列表中的证书不再会受到信任。

OCSP: 在线证书状态协议是一个用于获取 X.509 数字证书撤销状态的网际协议,作为证书撤销列表的替代品解决了在公开密钥基础设施建设中使用证书撤销列表而带来的多个问题。

可信平台模块 (“TPM”): 安全密码处理器的国际标准,可防止黑客尝试捕获密码、加密密钥和其他敏感数据。

可信密码模块 (“TCM”): 可信计算平台的硬件模块,为可信计算平台提供密码运算功能,具有受保护的存储空间。

Token: 经国家密码主管机构审批通过或经认证符合 FIPS 140-2 Level 2 或更高级别密钥存储硬件介质。

硬件安全模块 (“HSM”): 经国家密码主管机构审批通过或经认证符合 FIPS 140-2 Level 2 或更高级别硬件安全模块设备。

CA/浏览器论坛 : 它是一个证书颁发机构、浏览器软件供应商、操作系统 , 以及其他采用 PKI 的应用程序的自愿联合体, 为浏览器和证书颁发机构提供互联网安全行业标准。

UniTrust 证书策略 (“CP”): 本政策的最新版本可以通过访问 <https://www.sheca.com/repository> 获取。

UniTrust 证书认证业务规则 (“CPS”): 本政策的最新版本可以通过访问 <https://www.sheca.com/repository> 获取。

UniTrust TLS 证书认证业务规则 (“ TLS CP/CPS ”): 本政策的最新版本可以通过访问 <https://www.sheca.com/repository> 获取。

发行和管理公共可信证书的基线要求 (“BR”): Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates , 本文档最新版本可以通过访问 <https://cabforum.org/baseline-requirements-documents> 获取。

发行和管理 EV 证书准则 (“EV Guidelines”): Guidelines For The Issuance And Management Of Extended Validation Certificates, 本文档最新版本可以通过访问 <https://cabforum.org/extended-validation> 获取。

发行和管理公共可信的代码签名证书的基础要求 (“CSBR”): Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates , 本文档的最新版本可以通过访问 <https://cabforum.org/working-groups/code-signing/requirements/> 获取。

发行和管理 EV 代码签名证书准则 (“EVCS Guidelines”): Guidelines For The Issuance And Management Of Extended Validation Code Signing Certificates , 本文档的最新版本可以通过访问 <https://cabforum.org/ev-code-signing-certificate-guidelines> 获取。

发行和管理公共可信的邮件签名证书的基础要求 (“SBR”): Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates , 本文档的最新版本可以通过访问 <https://cabforum.org/working-groups/smime/requirements/> 获取。

二. 证书的使用和权限

授权

自订户证书的生效日起, UniTrust 授权订户使用证书的权利。

证书的使用范围

订户应仅在授权使用的范围内使用证书 , 否则 UniTrust 不对使用证书产生的结果负任何责任。对于 S/MIME 证书, 订户仅应在订户证书中列出的邮箱上使用此证书。

三. UniTrust 提供的服务

证书撤销状态查询服务

UniTrust 提供证书撤销列表 (“CRL”) 和在线证书状态协议 (“OCSP”) 作为证书撤销状态的查询服务。

证书撤销服务

公共可信 UniTrust 证书的吊销严格遵循 CA/B Forum 的强制性要求, 无论证书应用于何种场景, UniTrust 均不接受任何形式的延迟吊销申请。

1、如果发生以下任一情形, SHECA 将在 24 小时之内撤销订户证书:

- 订户 (或其授权的代理人) 请求撤销证书, 并确定请求撤销者是订户本人;
- 由于证书的不当使用而违反国家的法律法规;
- 订户告知 CA 原证书申请并未被授权, 也没有意图后续补充授权;
- CA 有证据指明, 订户证书中公钥配套的私钥有泄露的风险, 或不再符合 CPS 中关于密钥长度及密钥参数设置和质量检查的要求 (具体请参见 CPS 6.1.5 和 6.1.6);
- CA 发现存在一种方式可以轻易计算订户证书中公钥配套的私钥;
- CA 有证据指明, SSL 证书中的域名或 IP 地址, 或是 S/MIME 证书中的域名或邮箱地址的认证不可信;

- 当 CA 机构发现或被告知订户签名软件中含有可疑代码的情况下，CA 机构可以撤销代码签名证书。

2、如果发生以下任一情形，SHECA 将在 5 天之内撤销订户证书：

- SHECA 获得证据，表明证书被误用；
- SHECA 发现证书的签发不符合 CP/CPS 的要求；
- SHECA 依据 CP/CPS 的要求撤销证书；
- 订户证书里的信息做了实质性的更改；
- SHECA 签发证书后发现证书持有者申请其证书时提供的资料存在虚假信息；
- 订户违背了 CP、CPS 及订户协议等规定的义务、陈述或担保、或者订户不再能履行相关协议规定的义务；
- 订户没有履行付费义务；
- 继续使用订户证书会对 SHECA 的商业信用和信任模式造成损害；
- 订户机构合法主体的身份发生变化、撤销或解散；
- 由于技术或标准演变可能导致依赖方或应用软件提供方产生不可能接受的风险；
- SHECA 依据 Baseline Requirements 签发 SSL 证书的权利已届满或被撤销或终止，除非 CA 已作出安排，继续维护 CRL/OCSP；
- SHECA 得知订户不再能合法使用证书中包含的邮箱、域名或 IP 地址，如法院或仲裁停止了域名注册商使用某域名的权限，或域名注册商与申请人之间的使用许可或服务协议终止了，或帐户持有人未能保持电子邮件地址或域名的活动状态；
- SHECA 了解到某通配符 SSL 证书被用于验证具有欺诈误导性质的域名；
- SHECA 得知用户的私钥被泄露，或者如果有明确证据表明用于生成私钥的特定方法有缺陷；
- 法律法规的相关规定或要求。

撤销原因代码 (CRL reasonCode) 说明

原因编码	代码值	描述
unspecified	0	通过省略原因代码来表示。如果 CRL 条目是针对技术上无法导致颁发的证书，则必须省略原因代码，除非 CRL 条目是针对受这些要求约束的订户证书，且在 2023-07-15之前撤销。
keyCompromise	1	表示已知或怀疑订户的私钥已被泄露。
affiliationChanged	3	表示证书中的主体名称或其他主体身份信息已经发生改变，但没有理由怀疑证书的私钥已经被泄露。
superseded	4	表示证书被替换，因为：订户已请求新的证书，CA 有合理证据表明不应依赖对证书中任何完全合格域名或 IP 地址的域授权或控制的验证，或者 CA 出于合规原因（例如证书不符合这些基本要求或 CA 的 CP 或 CPS）已撤销证书。
cessationOfOperation	5	表示证书到期前，证书所属网站已关闭，或证书到期前，订户不再拥有或控制证书中的域名。
certificateHold	6	如果 CRL 条目适用于 1) 受这些要求约束的证书，或 2) 不受这些要求约束的证书，并且是 A) 在 2020-09-30 或之后颁发的，或 B) 在 2020-09-30 或之后不早于 2020-09-30，则不得包含在内。
privilegeWithdrawn	9	表示订户方存在违规行为，但尚未导致密钥泄露，例如证书订户在其证书请求中提供了误导性信息，或未履行其在订户协议或使用条款下的重要义务。（该编码仅供 CA 选择）

适用于代码签名或 EV 代码签名的时间戳服务

UniTrust 提供免费的符合规定的适用于代码签名的时间戳服务，UniTrust 建议订户在为代码进行签名时添加时间戳签名。适用于 PDF 签名的时间戳服务 (AATL)。

UniTrust 提供收费的符合规定的适用于 PDF 文档签名的时间戳服务，PDF 签名证书的订户可以合理的使用该服务，但 UniTrust 保留暂停服务的权利。

四. 订户的义务

信息的准确性

订户应承诺并保证在申请证书以及在提供签发该证书所需的相关信息时都要向 UniTrust 提供准确、完整、可靠且无误

导性的信息。因故意或过失未向 UniTrust 提供真实、完整和准确的信息，导致 UniTrust 签发证书错误，从而造成相关各方损失的，由订户承担相应责任。

订户应声明并确认拥有证书中的电子邮箱地址、主题备用名称里所列的域名或 IP 地址的控制权，如果订户不再控制电子邮箱地址、域名或 IP 地址，则订户应及时通知 UniTrust。

密钥对生成

订户应使用可信的系统生成和保护密钥对并满足以下要求：

- 1.生成的密钥对密钥长度 RSA 算法不小于 2048 位、ECC 算法不小于 256 位；
- 2.确保提交给 UniTrust 的公钥与私钥正确对应。

对于公共可信的代码签名证书，订户应使用以下任一方法生成和保护密钥对：

- 1.使用可信平台模块生成和保护密钥对；
- 2.使用可信密码模块生成和保护密钥对；
3. 使用硬件安全模块生成和保护密钥对。

对于公共可信的 EV 代码签名证书或 Adobe 文档签名证书，订户应使用使用硬件安全模块生成和保护密钥对。在证书有效期内，订户必须能够向 UniTrust 提供证书所关联的密钥存储在硬件安全模块上的证明，否则 UniTrust 将撤销已签发的订户证书，造成相关各方损失的，由订户承担相应责任。

私钥保护

订户应采取一切合理且必要的措施，以确保能始终控制、不泄漏、妥善保管和通过授权才允许使用证书中公钥相对应的私钥（以及任何相关激活数据或设备，如：密码或 Token）。如订户保管不善导致数字证书遭盗用、冒用、伪造或者篡改，订户应当自行承担相应责任。

私钥的重用

订户不应使用将要或已经用于非代码签名证书中的公钥申请公共可信的代码签名或 EV 代码签名证书。

若订户已知私钥存在泄漏风险，则不应使用该私钥对应的公钥信向 CA 发起证书请求，并应及时告知 CA 私钥存在泄漏的风险。

防止滥用

订户应采取适当的网络或其他安全控制措施以防止私钥被滥用，如果存在未经授权访问私钥的情况，则 UniTrust 可以直接撤销该证书而无需事先通知。

证书接受

在申请人或申请人代表审核并验证证书内容的准确性之前，订户不得使用证书。在收到证书后的 30 天内未对证书内容提出异议，则视为该证书已被接受。

证书的使用

证书中公钥相对应的私钥应仅限于订户本身访问和使用，订户应对使用证书的行为及其后果负责。所有使用证书在网上交易和网上作业中的活动均视为订户所为，因此而产生的相应后果应当由订户自行承担。

证书不得转让、转借或转用。因转让、转借或转用而产生的相关后果应当由订户自行承担。

在任何情况下，证书都不得用于网络钓鱼攻击、欺诈或对恶意软件进行签名等非法活动及犯罪活动。订户只允许在证书中主题 备用名称里所列的域名或 IP 地址可以访问的服务器上安装 SSL/TLS 或 EV SSL/TLS 证书。订户不应有意使用证书对包含可疑代码的软件进行签名。如果使用证书对 PDF 文档进行签名，用户应保留 PDF 文档签名时的审批记录。

对于公共可信的 EV 代码签名证书，订户还应接受以下附加义务：

- 1.仅对符合最新版 EV CS Guidelines 要求的代码进行签名；
- 2.仅限所授权公司的业务。

报告和撤销

在发生本协议声明的将撤销证书的情形时，订户应配合 SHECA 在相应的时限内撤销已签发的证书。

UniTrust 根据 Cab/From 要求制定的大规模撤销计划（MRIP&TP）可通过资源网站 <https://www.sheca.com/repository> 获取。触发大规模撤销事件时，UniTrust 将立即启动大规模撤销计划，并同步

提供替换证书签发服务。订户应尽快完成证书切换，配合 UniTrust 在规定时限内撤销原证书。

公共可信 webPKI 证书必须满足 Baseline Requirements 的强制撤销时间要求，对于将证书用于关键基础设施服务的订户，如果无法按照“三、证书撤销服务”中列举的 24 小时/5 天撤销时限配合 CA 进行证书撤销，则应谨慎使用 UniTrust 公共可信证书，建议使用私有化 PKI 方案。

证书使用的终止

订户应在证书过期或撤销后立即停止使用与证书中公钥相对应的私钥。

响应能力

订户应在 48 小时内向 UniTrust 回应关于私钥泄露或证书滥用的情况说明。

承认和接受

如果订户违反本协议或使用条款，或 UniTrust 发现证书被用于非法活动、犯罪活动（如：钓鱼网站攻击、欺诈、发布恶意软件或为恶意软件进行签名），那么 UniTrust 有权立即撤销该证书。

信息共享

对于公共可信的代码签名或 EV 代码签名证书，UniTrust 可以在以下情况下将申请人的公开信息、订户证书、已签名的应用程序和相关情况分享给其他 CA 机构、行业组织和 CA/浏览器论坛：

- 1.证书或申请人被确认为可疑代码的来源；
- 2.无法验证申请证书的权利；
- 3.证书被撤销的原因并非订户主动请求（如：私钥泄露、为恶意软件签名等）。

符合行业标准

UniTrust 可以在必要的时候修订本协议以遵守 BR、Guidelines、MRCS 或 EVCS Guidelines 的任何变动。本协议修订后的版本将在网站上公布 30 天后生效，订户随时可以通过访问 <https://www.sheca.com/repository> 获取最新版本的订户协议。如果不同意修订，那么订户可以随时终止本协议，并要求 UniTrust 从协议终止之日起至证书服务到期日止按比例退款。

五. 信息发布

订户同意 UniTrust 使用以下方法公开披露申请证书时提供的信息：

- 1.信息嵌入证书中公布；
- 2.在证书透明度（Certificate Transparency）日志中公布证书。

六. 期限和终止

本协议自证书服务到期日起自动终止。以下情况本协议将提前终止：

- 1.双方协商一致同意提前终止；
- 2.订户未能履行本协议中的义务，并且订户在收到 UniTrust 通知后的 30 天内未能进行有效纠正。

本协议终止后，本协议第二条授予订户的权利将被终止，UniTrust 可以根据证书撤销程序撤销订户证书，订户应履行证书使用的终止义务停止使用证书。本协议的终止不影响本协议第四、五、六、七、八、九、十一条款的有效性，上述条款将继续有效以允许必要的义务得到充分执行。

七. 免责声明

除 CPS 声明的内容外，本协议相关的证书服务均以实际服务为准。SHECA 及其分支机构、授权方不就证书服务的完整无误、内容安全及其他任何损失做任何明示、暗示、法定或其他形式的担保或声明。SHECA 及其分支机构、授权方仅承担法律规定的义务，拒绝承认任何其他担保，包含适销、品质、特定用途适用的默认担保，无侵权声明，保密权，及商业管理或交易习惯衍生的担保。

八. 责任限制

SHECA 及 SHECA 分公司或授权方均不就任何间接、附带、特殊、后果性或惩罚性损害（包括但不限于利润、商誉、

使用或数据损害) 向您承担责任, 即使一方已被告知该等损害发生的可能性, 且即使该等损害已被预见。此外, SHECA 及 SHECA 分公司或授权方也不会就与下述内容有关的赔偿、补偿、损失负责:

1. 您无法使用证书, 该情况可能因下述原因导致;
 - a) 本协议终止或暂停或证书仍然处于批准程序或被撤销;
 - b) SHECA 停止运营本协议部分或全部服务;
 - c) 因任何原因(包括停电、系统故障或其他中断)导致的任何证书服务全部或部分的关闭。
2. 因购买替换性商品或服务产生的费用;
3. 你所产生的与本协议相关的因使用 UniTrust 证书服务或拥有相关权限而发生的其他投资、支出或义务;
4. 任何未经授权访问、更改、删除、销毁、损坏、丢失或未能存储您的任何内容或其他数据。

任何情况下, SHECA 及 SHECA 分公司或授权方与本协议及其约定下证书有关的总计责任应低于您在证书签发期间为证书支付的金额。为避免争议, 尽管有前述约定, 就本协议约定下签发的任何增强型证书, SHECA 及 SHECA 分公司或授权方的总计责任将被限制为每张增强型证书 20000 元人民币。

九. 知识产权

本协议任何一方, 均不能通过签署和履行本协议获得对方的任何知识产权(包括但不限于商标、标识、专利、著作权、技术秘密、数据等); 除非拥有知识产权的一方以书面方式授予了使用该等知识产权的许可, 否则另外一方也无权使用该等知识产权。订户不得基于本协议以任何方式、主张、理由寻求 SHECA 就其提供的全部软件、程序、文档、系统、数据的任何知识产权。在 SHECA 提供服务过程中存在、产生、包含任何知识产权均受到法律保护, 未经 SHECA 的书面授权许可, 任何人不得基于该等知识产权以任何形式予以使用、创作衍生品或将其商业化。

十. 协议完整

以下政策及其更新的版本通过引用纳入本协议:

- UniTrust 证书认证业务规则;
- UniTrust TLS 证书认证业务规则;
- 发行和管理公共可信证书的基线要求;
- 发行和管理 EV 证书准则;
- 发行和管理公共可信的代码签名证书的基础要求;
- 发行和管理 EV 代码签名证书准则。
- 发行和管理公共可信的邮件证书的基础要求

十一. 法律适用、管辖与其他

本协议之订立、生效、解释、修订、补充、终止、执行与争议解决均适用中华人民共和国大陆地区法律。因本协议产生的争议, 首先应友好协商解决。协商不成时, 任何一方均可向 UniTrust 住所地有管辖权的人民法院提起诉讼。

本协议任一条款被视为废止、无效或不可执行, 该条应视为可分的且并不影响本协议其余条款的有效性及其可执行性。

本协议的最终版本以中文撰写。如果本协议被翻译成其他任意一种语言并且中文版本和翻译版本之间存在冲突, 则以中文版本为准。(正文完)