万维信 EV 代码签名证书订户协议

甲方：

地址：

邮政编码：

乙方：上海市数字证书认证中心有限公司

地址：上海市四川北路 1717 号 18 楼

邮政编码：200080

为了确保万维信 EV 代码签名证书得到安全、可靠、妥善、适当的使用，上海市数字证书认证中心有限公司（以下简称甲方，缩写为 SHECA）与_____（以下简称乙方）签订本订户协议（以下简称本协议），就申请、接受或使用万维信 EV 代码签名证书进行约定。具体内容包括：

一、本协议相关名词定义

证书申请：是指向认证机构请求签发数字证书。

认证机构（CA）：签发、挂起、撤销数字证书的电子认证服务机构，本协议中特指 SHECA。

订户：指拥有数字证书的个人、组织等实体，有能力并被授权使用与证书中公钥相对应的私钥，本协议中仅指各类组织，不包括个人。

代码签名证书：由认证机构签发，用于验证由软件发布方提供的代码的完整性，并标明和识别软件发布方的身份。

电子认证业务规则（CPS）：认证机构在签发、挂起、撤销证书时所遵循的规范，该规范需要不断更新，并对外公布，通常发布在认证机构网站的知识库中。

知识库（Repository）：认证机构通过 Web 方式对外发布相关文档、证书等内容的资源库，通常是网页链接的集合。

依赖方：指依赖数字证书或数字签名的个人或组织。

二、乙方在申请、接受或使用万维信 EV 代码签名证书之前，请仔细阅读本协议。在要求颁发万维信 EV 代码签名证书之前，双方要保证本协议已经被正确的签署，并且以同意和接受本协议作为申请证书的条件。如果乙方已经使用了该数字

证书，就表明乙方同意接受本协议所规定的所有条款。如果乙方不同意本协议或本协议中的任何一个条款，请立即向 SHECA 归还尚未使用的证书，乙方将得到全额退款。如果乙方在理解本协议上有任何疑问，请通过电子邮件 legal@sheca.com 进行联系。

三、双方同意本协议适用于万维信 EV 代码签名证书。该证书是按照 SHECA 的《EVSSL 证书电子认证业务规则（CPS）》（以下简称 CPS，可在 www.sheca.com 获取）的规定来签发的，该 CPS 遵循《CA/浏览器论坛增强认证证书指南》（《CA/BrowserForumGuidelinesforExtendedValidationCertificates》，以下简称指南，可在 www.cabforum.org 获取）要求，并将其作为参考资料编入其中。双方均同意和接受《指南》中规定的有关 EV 代码签名证书颁发和管理的强制性措施。

四、乙方申请和持有的万维信 EV 代码签名证书，仅能用于乙方发布的合法软件或代码中，并且必须符合法律法规的规定。乙方禁止在知情的情况下签署任何含有可疑代码的软件。并且，在使用 EV 代码签名证书时，乙方保证：

1、不为或不代表任何其他组织使用

2、不以证书申请时提交的组织名称以外的任何名称执行私钥或公钥操作

3、不发布有害或恶意内容，包括但不限于可能会对接受者产生不利影响的内容；

4、不在危险环境作为控制设备使用，也不能用于任何可能导致人身安全、环境破坏的应用中。

五、在本协议生效且在用户完成了相关付款义务后，SHECA 将提供以下服务：

1、乙方按照要求完成资料提交等申请过程后，SHECA 将根据 CPS 的规定处理该申请，符合要求的将会签发证书并提供给乙方。乙方在下载证书或以其它方式安装证书时，需要对证书内容进行核对，申请人或申请代理人检查并验证证书内容准确无误之前不得使用证书，并保证发现有任何问题时会尽快联系 SHECA。SHECA 会撤销包含问题内容的证书并重新签发一个新的证书。

2、SHECA 将尽合理努力，使相关各方可以查询、验证和获取当前有效的 CRL。但由于超出 SHECA 合理控制范围的设备故障、设备维护造成的中断或通讯中断等因素导致的 CRL 服务滞后或不能提供，不能被视作 SHECA 没有履行该义务。

3、SHECA 发现或者有理由确认乙方的私钥存在安全隐患，或数字证书被盗用，乙方应根据 SHECA 的要求在规定的时间内作出回应。发生下列下列情形之一的，SHECA 可撤销其发放的 EV 代码签名证书：

- 发现乙方证书中的信息失效
- 有证据表明乙方将该证书用来签署恶意代码或其它违法法律规定的使用
- 乙方无法履行或违背了 CPS 里规定的实质义务；
- 继续使用该证书将会对 SHECA 或其他方利益遭到损坏；
- 证书里的主题信息已经修改；
- 用户应采取适当的网络和其他安全控制保证私钥不会被滥用误用，否则 SHECA 在发现用户私钥在未授权情况下被盗用时，有权在通知订户前立即吊销此证书。
- SHECA 通过单方面的考虑，发现 EV 代码签名证书的颁发没有遵循《指南》或 SHECA 的 CP/CPS；
- SHECA 终止营运并且尚未安排另外的 EV 证书签发机构来提供 EV 代码签名证书的撤销支持服务；或者 SHECA 不再具备签发 EV 代码签名证书资质；
- 用户应保证遵守用户协议，否则 SHECA 有权立即吊销此证书。
- 法律法规规定的其他情形。

六、SHECA 确保不会因在证书生成时的失误导致乙方证书内的信息发生错误，证书签发、更新等完全遵循 CPS 规范的要求，证书撤销、挂起和知识库的使用符合 CPS 规范。

SHECA 将按照法律法规和 CPS 的要求处理乙方提交的信息，并公开发布证书及证书相关信息。

七、乙方确保接受以下事项的约束，并履行相应的义务：

1、承诺并保证在任何时候都要向 SHECA 提供准确的、完整的信息。这包括在申请 EV 代码签名证书时，以及在 SHECA 要求提供与签发该证书所需的相关信息时。在证书申请信息发生变更或失效时，应及时通知 SHECA。

确保明确地授权证书批准人（Certificate Approver）在申请 EV 代码签名证书时，可以行使以下权限：

（1）代表乙方提交或授权申请经办人（Certificate Requester）提交 EV 代码签名证书请求；

（2）为颁发 EV 代码签名证书，提供或授权申请经办人提供有关用户信息；

（3）批准由申请经办人提交的证书申请。

2、向 SHECA 提交的信息（包括 email）不会侵犯任何第三方的知识产权，不能包含有违法法律或侵犯任何一方合法权益的材料，并且不会用于任何非法目的。
3、在申请证书时，乙方应按照 SHECA 公布的收费标准支付证书相关费用。在证书签发后的 30 日内，如果对证书不满意的，可以提出申请退款。SHECA 将在撤销该证书后返还相应款。超过 30 天的，除非 SHECA 违反本协议规定或有其它重大责任，乙方才有权要求退款。

3、为保证签发 EV 代码签名证书，要使用可信系统并按照可靠流程来产生其私钥和公钥，确保使用被公认为适合用于电子签名的算法来产生密钥，并采用被公认为适合用于电子签名的密钥长度。

4、采取必要的、合理的措施来保持对与其申请的 EV 代码签名证书里与公钥相匹配的私钥（以及相关权限信息和装置，如密码和令牌）总是具有专有控制权、并进行保密和妥善保护，并采取合理的预防措施来防止私钥的遗失、泄露、被篡改或被未经授权使用，任何未经授权的人将不能获得这些信息。同时，要保证其提交给 SHECA 的公钥与其使用的私钥正确匹配。

5、在安装和使用 EV 代码签名证书前，申请人或申请代理人要认真、仔细确认该证书中信息的正确性。在收到 EV 代码签名证书后 7 天内没有做出任何反应，SHECA 就认为证书已经被接受。

6、应当并且只能将 EV 代码签名证书用于合法目的，并且遵循本协议的使用规定；作为订户证书，不得将其用于签发证书、CRL 及其它相关信息；保证使用证书对应的私钥所创建的数字签名就是乙方做出的数字签名，在签名时证书未过期或且未被撤销。

7、在下列情形下，乙方要立即停止使用 EV 代码签名证书以及其对应的私钥，并立即要求 SHECA 撤销该证书：

- 确认或怀疑证书及证书有关的私钥正受到不正确使用、损坏或私钥丢失；
- 原来的 EV 代码签名证书申请是未得到授权或不能追溯到授权；
- 乙方名称发生变更
- 证书里的需要认证的信息不正确、已经改变，或与用户申请证书时提交的信息不符；
- 本协议已经终止；

- **有证据表明证书被用于签发可疑代码。**

8、乙方保证不对 SHECA 的证书系统进行破坏、干扰和反向侦测。

9、作为依赖方时，应保证有足够的信息来判断是否信赖或在多大程度上信赖一张数字证书，并依据上述信息自行作出决定。同时应承认接受 SHECA 发布的依赖方协议的约束。如果未履行依赖方义务，乙方将自行承担相应损失，对第三方造成损失的，应承担赔偿责任。

10、一旦 EV 代码签名证书过期或被撤销后，乙方要立即停止使用与该 EV 代码签名证书里所列公钥相配的私钥，并从设备上卸载该证书，证书到期或撤销后用户私钥不能再使用。

11、如果：1）证书或证书申请者被确认为可疑代码源；2）申请证书的机构无法核实；3）证书因出用户要求以外的缘故被吊销，SHECA 将有权对外披露给其他 CA 机构或行业组织。

12、如果乙方的下列行为造成了 SHECA 或其他第三方的损失，乙方同意对进行相应赔偿：

- 违反了本协议规定的权利和义务内容；
- 证书申请时捏造或者歪曲事实；
- 所提供的信息侵犯了第三方的知识产权；
- 有误导性地陈述事实或有意欺骗对方；
- 根据本协议条款，未使用可靠的系统，或未采取必要的预防措施以防止私钥损坏、泄露、未经授权使用等。

本协议中止或终止时，本条款将继续有效。

八、乙方同意 SHECA 通过 CRL、OCSP 或 HTTP 方式公布其 EV 代码签名证书或证书序列号等相关信息。

九、在任何情况下（除非是欺诈或犯罪行为），SHECA 不会对证书、数字签名或其它 CPS 规定的其它交易或服务进行使用、交付、许可、执行或不执行而造成的任何间接的、偶发的、结果性的损害承担任何责任，也不会因乙方使用证书、数字签名等造成的任何利润的损失、数据丢失或其它间接的、偶发的、结果性的损害承担任何责任。除非是由于 SHECA 的原因造成证书被错误签发、CRL 服务无法被验证时，用户在信赖证书时造成的上述损害，SHECA 将进行赔偿。SHECA 对一张 EV 代码签名证书赔偿的限额为 300，000 元人民币（45,000 美元）。如果是乙方的欺诈、犯罪或其他行为造成证书信赖的错误时，SHECA 将

不对上述情况承担任何责任，并保留追索相关赔偿的权利。如果依赖方没有遵守履行由 CPS 和本协议所规定的义务时，SHECA 也将不对上述情况承担任何责任。

十、本协议从有效日开始起有效，直至乙方证书过期或被撤销。协议有效期一般为 1 年，到期后自动终止；在有效期内，如果乙方没有履行本协议规定的实质性义务，且在接到 SHECA 的通知后 30 天内没有进行有效纠正，本协议将自动终止。本协议任何条款被具有司法管辖权的法院判定无效或无法履行，并不影响其余条款的有效性和可执行性。

十一、无论何种原因，一旦本协议终止，乙方的 EV 代码签名证书将会被 SHECA 按照程序撤销并立即生效。一旦 EV 代码签名证书被吊销，乙方依据本协议第三条所获得得权限也将同时被终止。但这样的终止将不影响本协议第五、六、七条和第九、十、十一、十二、十三、十四、十五、十七条的有效性，上述条款将继续有效以允许必要的义务得到充分执行。

十二、本协议将按照中华人民共和国的相关法律来进行解释。协议履行过程中发生争议的，如协商不成，双方同意提交协议签订地人民法院裁判；除非另有说明，本协议将产生约束效应，并对后任人、执行者、继承人、代表、管理人和双方的指派人的利益产生法律效力；乙方不能转让本协议及其数字证书，任何这样的有意转让或委派都是无效的，一旦发生此种情形，SHECA 有权终止本协议；本协议优先于双方所有之前的口头或书面的约定。

十三、当乙方希望或被要求提供关于本协议的告示、需求或请求给 SHECA 时，所有的通讯联络必须是书面的，而且必须以能够保留收据并且要求收件人收到后返回回执的快递服务寄到下列地址：

上海市四川北路 1717 号 18 楼战略发展部收
上述的通讯联络在收到后即生效。

十四、SHECA 可能会使用适当的第三方数据库来验证申请过程中的诸如姓名、地址和其它个人资料，以及机构注册信息、机构地址等。通过接受本条款，乙方就同意了接受此类审查。在实施这样的审查时，证书申请的相关自然人所提供的个人信息可能会提交给有关机构并有可能被保存下来。这样的审查仅用来确认身份而不会用作它途，不会对相关自然人的信用等造成影响。

十五、由于签署和履行本协议，本协议双方并不能获得对方的商标、品牌、图标和产品指定的权利，也无权使用这类资料，除非拥有这些资料所有权的一方以书面的形式授权了对方，对方才能使用。

十六、SHECA 有权修改本协议的条款，或随时改变所提供的服务的一部分。SHECA 可以根据国际 CA 标准及要求的变化调整本协议的相关内容。协议的修改将会在 SHECA 网站上公布 30 天后或通过 e-mail 通知乙方时生效。如果乙方不同意修改，可随时终止本协议，并要求 SHECA 从协议终止之日到服务结束时按照比例退款。如果乙方在变更后继续使用 SHECA 提供的证书或相应服务，即表示乙方遵守新的协议并受其约束。

十七、乙方同意微软公司（Microsoft）作为本协议的第三方利益相关人。

十八、本协议一式两份，具有同等法律效力。

注：SHECA 时间戳服务器严格按照国际标准 RFC3161 进行配置部署，上海 CA 郑重推荐您使用 SHECA 时间戳对签名代码进行时间戳认证。

甲方：

地址：

授权签署人：

签署日期

乙方：上海市数字证书认证中心有限公司

地址：上海市虹口区四川北路 1717 号嘉杰国际广场 18 楼

授权签署人：

签署日期：