欧利斯认证有限公司
数字资产服务认证技术规规范

受控状态：受控

文件编号：**CTS OLS/GZ-0247-2025**

发布日期：**2025-07-15**

实施日期：**2025-07-15**

版本/版次：**A/0**

编制部门：技术开发部

评审人： 蒲文雄

批准人： 沈育谦

文件制/修订履历

制/修订日期	制/修订单号	制/修订类别	版本/版次	制/修订说明（原因、内容见制修订审批单）
2025-07-15	初始制订	■制订 □修订	A/0	初始发布、实施

前 言

本认证标准是欧利斯认证有限公司开展数字资产服务认证的依据。

本认证标准为首次发布。

本认证标准由欧利斯认证有限公司组织制定。

本认证标准主要起草人：沈育谦、蒲文雄。

本认证标准自 2025 年 7 月 15 日起正式实施。为确保平稳过渡，对于已通过清洁行业企业资质评价体系认证的组织，以及在 2025 年 10 月 15 日前已提交评审申请的企业，给予 1 年过渡期，须于 2026 年 10 月 15 日前完成体系改版及重新认证工作，逾期未完成的，原认证资格将自动失效。

本认证标准由欧利斯认证有限公司解释。

目录

1 范围

本认证适用于各类所有制的数字资产服务机构（含国有企业、民营企业、外资企业等），涵盖数字资产存储、交易、托管、评估、确权、清算等服务业态，评价机构在数字资产服务合规性、安全性、技术能力、客户权益保障等方面的管理水平与服务质量。不适用于个体数字资产从业者、非服务类数字资产研发企业及非法数字资产相关机构。

2 引用标准

1. 《中华人民共和国网络安全法》：明确网络运营者（含数字资产服务机构）的网络安全保护义务，是数字资产服务网络安全管理的根本法律依据。
2. 《中华人民共和国数据安全法》：规定数据（含数字资产相关数据）收集、存储、使用、加工、传输等环节的安全要求，为数字资产数据安全保障提供法律支撑。
3. 《区块链信息服务管理规定》（国家互联网信息办公室令第 3 号）：明确区块链信息服务（含基于区块链的数字资产服务）的备案、技术安全、内容安全等要求，是区块链类数字资产服务合规运营的核心准则。
4. 其他相关的国家、行业标准及法律法规：包括密码安全（如《信息安全技术 密码应用基本要求》GB/T 39786-2021）、个人信息保护（如《中华人民共和国个人信息保护法》）、反洗钱（如《金融机构反洗钱规定》）等方面的标准和法规，确保数字资产服务全方位合规，保障客户、机构及社会公众的权益。

3 术语和定义

1. 数字资产：指以电子数据形式存在，具有价值属性和可交易性的资产，包括但不限于虚拟货币（合规范围内）、数字藏品、区块链资产、电子债权凭证等。
2. 数字资产服务：数字资产服务机构为客户提供的数字资产存储、交易撮合、资产托管、价值评估、权属确认、清算结算等专业化服务。
3. 数字资产安全管理：机构通过技术防护（如加密、防火墙）、制度管控（如权限管理、操作日志）、应急处置等方式，防范数字资产被盗、篡改、丢失及网络攻击的管理活动。

4. 客户权益保障：机构通过合规服务、信息披露、风险提示、纠纷处理等措施，保障客户在数字资产服务过程中的资产安全、知情权、公平交易权等合法权益.

5. **认证**：由具备公信力的第三方认证机构证明数字资产服务机构符合特定数字资产服务标准或技术规范的合格评定活动，增强机构在市场中的可信度和竞争力。

4 数字资产服务机构资质要求

4.1 基础合规性

1. 依法取得营业执照、相关行业主管部门备案 / 许可文件（如区块链信息服务备案编号、金融相关业务许可 <若涉及>），证照及备案文件在有效期内，无超范围经营行为。
2. 建立健全数字资产服务合规管理体系，明确合规管理部门及岗位职责，配备至少 2 名专职合规人员（机构员工人数不足 10 人的可配备兼职合规人员），合规人员需具备数字资产、网络安全、法律法规相关专业背景或从业经验。
3. 严格执行反洗钱与反恐怖融资要求，建立客户身份识别（KYC）、交易记录保存、大额及可疑交易监测与报告机制，客户身份识别覆盖率达 100%，交易记录保存期限不少于 5 年。

4.2 服务管理制度

1. 建立健全数字资产服务管理体系：涵盖数字资产存储管理制度（含加密密钥管理）、交易服务规则、托管服务流程、评估标准、确权操作规范、客户信息管理制度、风险控制制度等，制度内容符合法律法规及行业标准要求，并向客户公示服务流程、收费标准、风险提示。
2. 制定服务风险防控机制：定期（每季度至少 1 次）开展数字资产服务合规自查与风险评估，排查技术安全、客户身份识别、交易合规等环节的风险点，建立风险台账并及时整改，留存自查与整改记录。

3. 建立客户沟通与信息披露机制：设立 24 小时客户服务热线、线上反馈渠道（如 APP、官网客服），保障客户诉求 48 小时内响应；定期（每月至少 1 次）向客户披露数字资产服务运营情况（如系统维护计划、资产托管状态），重大风险事件（如系统漏洞、资产异常变动）需在 24 小时内告知受影响客户。

4.3 技术安全要求

1. 数字资产存储安全：采用符合国家密码标准的加密技术（如对称加密、非对称加密）对数字资产及客户信息进行加密存储；核心资产采用 “冷钱包 + 热钱包” 混合存储模式，冷钱包存储比例不低于总托管资产的 70%，冷钱包需离线存放并建立多重权限管控。
2. 系统安全防护：搭建符合《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）二级及以上标准的网络安全防护体系，配备防火墙、入侵检测系统（IDS）、数据备份与恢复系统，系统漏洞扫描频率不低于每月 1 次，数据备份采用 “本地 + 异地” 双备份模式，备份恢复成功率达 100%。
3. 操作安全管理：建立数字资产服务操作权限分级制度，不同岗位设置差异化操作权限，关键操作（如资产转移、密钥使用）需实行 “双人复核”；完整记录所有操作日志（含操作人、时间、内容、结果），日志保存期限不少于 5 年，且不可篡改。

4.4 客户权益保障

1. 风险提示与告知：在服务开通前，向客户出具书面风险提示书，明确数字资产服务的市场风险、技术风险、政策风险等，客户确认签字后方可提供服务；服务过程中若风险等级发生变化，需及时更新风险提示并告知客户。

2. 资产隔离与确权：客户数字资产与机构自有资产严格隔离存储，单独核算，不得挪用客户资产；建立数字资产权属确认机制，通过区块链存证、权属证明文件审核等方式明确资产归属，确权准确率达 100%。

3. 客户信息保护：遵循最小必要原则收集客户信息，不得收集与服务无关的信息；采用加密、访问控制等技术保护客户信息，禁止向第三方泄露客户信息（法律法规要求除外），客户信息泄露事件发生率为 0。

4.5 人员管理与培训

1. 人员资质：数字资产服务核心岗位（如技术开发、安全运维、交易审核、合规管理）人员需具备数字资产、网络安全、金融科技相关专业背景或 1 年以上相关从业经验；关键岗位人员（如密钥管理员、风控负责人）需通过背景审查，无犯罪记录及不良从业记录。

2. 保密管理：与全体员工签订保密协议，明确数字资产、客户信息、技术架构等保密内容及违约责任；核心岗位人员需额外签订竞业限制协议（若涉及），离职后竞业限制期限不超过 2 年。

3. 年度培训：建立年度员工培训计划，培训内容涵盖数字资产服务合规要求、技术安全防护、反洗钱操作、客户权益保障、应急处置等，每人每年培训时长不低于 30 小时，留存培训签到、课程资料、考核结果等记录；新员工入职培训时长不少于 16 小时，培训合格后方可上岗。

4.6 纠纷处理与应急

1. 建立客户纠纷处理机制：设立专门的纠纷处理部门或岗位，明确纠纷申请、调查、处理、结果反馈等环节的时限与要求，一般纠纷需在 7 个工作日内完成处理，复杂纠纷不超过 30 个工作日；处理结果需经客户确认，留存纠纷记录与处理档案。

2. 制定应急处置预案：针对数字资产被盗、系统瘫痪、网络攻击、政策变更等突发事件制定应急预案，明确应急组织架构、处置流程、责任分工；每半年至少组织 1 次应急演练（如模拟系统被攻击、资产异常转移），留存演练记录与影像资料，应急预案更新频率不低于每年 1 次。

3. 近 3 年内无重大服务纠纷事件（如群体性客户投诉、客户资产重大损失），无因违规服务、安全漏洞引发的负面舆情或监管处罚。

4.7 服务质量与满意度

1. 服务响应时效：客户服务请求（如咨询、问题反馈）响应时间不超过 2 小时，技术故障（影响服务正常运行的故障）修复时间不超过 4 小时，重大故障（如系统瘫痪、资产无法访问）修复时间不超过 24 小时。

2. 服务准确率：数字资产存储、交易、托管等服务操作准确率达 99.9% 以上，因机构操作失误导致的客户资产损失需在 72 小时内完成赔付或补救。

3. 客户满意度调查：每年至少 2 次通过问卷调查、一对一访谈等方式，收集客户对服务合规性、资产安全性、响应及时性、纠纷处理效果等方面的满意度反馈，客户满意度不低于 85%，并针对调查结果制定改进措施，留存调查与改进记录。

5 认证模式

采用 “文件审核 + 现场审核 + 客户满意度调查 + 持续监督” 的综合认证模式。

1. **文件审核**：对数字资产服务机构提交的服务管理制度、合规备案文件、技术安全方案、人员培训档案、纠纷处理流程等进行审查，判断机构是否满足数字资产服务认证的基本文件要求，评估制度合规性与完整性。
2. **现场审核**：认证机构派遣审核员到机构现场，检查机构实际运营情况（如客户身份识别记录、交易日志、冷钱包存储管理、系统安全防护设施）、员工服务规范、应急处置演练记录等，验证实际服务与标准的符合性。
3. **客户满意度调查**：通过随机抽样（抽样比例不低于机构近 3 个月客户总量的 5%），采用问卷调查、一对一访谈等方式，收集客户对资产安全、服务合规、响应时效、纠纷处理等方面的满意度反馈，客户满意度

需达到 85% 以上（含 85%），未达标机构需分析原因并整改，认证机构复查确认。

4. **持续监督：**证书有效期内，认证机构每年开展 1 次监督审核，检查机构数字资产服务的持续合规性、客户满意度变化、安全事故与纠纷处理情况等。发现一般不符合项，机构需在 30 日内整改；发现严重不符合项（如证照 / 备案失效、重大安全漏洞、客户资产挪用），暂停或撤销认证证书。

6 认证流程

申请受理

1. 企业向认证机构提交正式书面认证申请，同时需一并提交企业营业执照、相关行政许可证明（若有）、企业简介、服务范围说明、管理制度文件、人员资质证书、设备清单、服务案例合同等详实申请材料。
2. 认证机构在收到申请材料后的 5 个工作日内，对申请材料进行初步审查，确定是否受理申请。如申请材料存在不完整或不符合要求的情况，及时通知企业补充或修改材料。

文件审核

1. 认证机构组织审核员对受理企业的申请材料开展详细文件审核，审核内容全面涵盖企业的组织架构、人员配备、管理制度、服务流程、设备管理、应急预案、服务案例等是否符合对应资质等级标准要求。
2. 文件审核完成后，审核员出具专业的文件审核报告，明确指出企业存在的不符合项。企业需在规定时间内对不符合项进行认真整改，并提交整改报告。认证机构对整改报告进行严格验证，确认整改有效后方可进入现场审核阶段。

现场审核

1. 认证机构与企业协商确定现场审核时间，提前 7 个工作日向企业发出现场审核通知。审核组由具有相应资质和丰富经验的审核员组成。
2. 现场审核严格依据相关标准和企业申请认证范围，对企业的经营场所、服务项目现场进行全面、细致检查。审核内容包括但不限于人员操作规范、设备设施状况、服务质量控制、环境卫生保护、安全管理措施、客户服务等关键方面。

3. 现场审核过程中，审核员认真记录发现的不符合项，并与企业相关人员进行充分沟通确认。现场审核结束后，审核组召开末次会议，向企业通报审核结果，明确提出不符合项整改要求。

客户满意度调查

1. 在现场审核前后，认证机构通过随机抽样方式，选取一定数量具有代表性的企业服务客户进行满意度调查。调查内容全面涵盖服务质量、服务态度、响应及时性、问题解决效果等方面。

2. 对客户满意度调查结果进行科学统计分析，客户满意度需达到［具体满意度数值］以上，否则企业需深入分析原因并采取切实有效的改进措施，认证机构视情况进行复查。

认证决定

1. 认证机构根据文件审核、现场审核和客户满意度调查结果，对企业是否符合认证要求进行综合评价。经认证机构技术委员会审议，作出认证决定。

2. 对符合认证要求的企业，颁发相应等级的证书，证书有效期为 3 年。对不符合认证要求的企业，认证机构向企业出具不予认证通知，详细说明原因，并告知企业可在整改完成后重新申请认证。

持续监督

1. 在证书有效期内，认证机构每年对获证企业进行至少一次监督审核。监督审核内容包括企业认证范围内服务的持续符合性、管理体系运行有效性、客户反馈情况、是否有重大变更等。

2. 监督审核发现企业存在一般不符合项，企业需在规定时间内完成整改，认证机构对整改情况进行验证。如发现严重不符合项或企业出现影响认证有效性的重大问题，认证机构将视情况暂停或撤销企业认证证书。