芬兰（MiCA）加密资产服务提供商（CASP）牌照

常见问题（FAQ 大全）

本文依据 **MiCA 最新法规 + 芬兰监管机构 FIN-FSA（芬兰金融监管局）** 的本地化要求**由 仁港永胜（香港）有限公司 拟定，并由 唐生 提供专业讲解。**

内容可直接用于：

- 内部立项
- 投资人沟通
- 监管面谈准备
- MiCA 项目申报文件
- 合规制度建设
- RFI 回答草稿

牌照名称：芬兰加密资产服务提供商牌照 Crypto-Asset Service Provider（CASP）
服务商：仁港永胜（香港）有限公司

✅ 点击这里可以下载 PDF 文件：芬兰加密资产服务提供商（CASP）牌照申请注册指南
✅ 点击这里可以下载 PDF 文件：关于仁港永胜

芬兰（MiCA）加密资产服务提供商（CASP）牌照常见问题（FAQ大全）

Crypto-Asset Service Provider (CASP) under MiCA — Finland Version
Compiled by Rengangyongsheng (Hong Kong) Limited · Explained by Mr. Tang Shangyong

---

第一章｜基础概念与芬兰 MiCA 实施情况（Q1～Q40）

（本文所有内容为监管实操标准，适用于直接交付 FIN-FSA 或内部立项文件）

Q1：什么是 MiCA？为什么芬兰必须执行？

MiCA（Markets in Crypto-Assets Regulation）是欧盟统一加密资产监管框架。
自 2024 年起所有欧盟成员国（包括芬兰）必须强制执行。

芬兰并没有自己的"本地加密法"，而是严格对齐 MiCA。

Q2：芬兰 CASP 的监管机构是谁？

FIN-FSA（Financial Supervisory Authority）
是芬兰全部金融许可的主管单位，包括 MiCA、EMI、PI、投资公司等。

Q3：MiCA 适用于哪些加密服务？

MiCA 共 8 项 CASP 服务均适用：

1. 接收与传送
2. 执行订单

3. 自营交易
4. 托管与钱包管理
5. 交易平台运营
6. 投资建议
7. 组合管理
8. 放贷/借贷/加密组合管理服务（视类别细化）

Q4：是否所有加密企业都必须申请芬兰 CASP?

在芬兰设立机构且提供 MiCA 监管服务 → 必须申请。
在芬兰无实体但向芬兰客户推广 → 仍受管制。

Q5：MiCA 在芬兰的最大特点是什么?

3 个关键词：

- **极其严格的 AML（完全对齐芬兰 AML 法）**
- **极强的金融消费者保护文化**
- **IT 与安全要求偏高（北欧系统稳定性要求高）**

Q6：芬兰是否对交易所（Platform）类业务特别严格?

是的。
交易平台类（Matching Engine）将被 FIN-FSA 视为"系统性风险"。
审查深度类似传统金融市场基础设施。

Q7：芬兰是否接受纯线上公司申请（无实体）?

不接受。
必须有本地实质（办公室 + 人员）。

Q8：芬兰是否强制要求本地管理层?

必须至少：

- 本地董事 1 名
- 本地 AML 报告官（MLRO）
- 实体办公地点

Q9：芬兰 CASP 牌照可否跨境护照?

可向欧盟 27 国 + EEA 3 国（挪威、冰岛、列支敦士登）护照展业。

Q10：芬兰是否允许白标系统申请 MiCA?

允许，但 FIN-FSA 会要求：

- SLA
- 授权证据
- 明确的可审计性

Q11：MiCA 是否允许芬兰企业托管客户资产?

可托管，但要求极高：

- 冷热分层
- MPC/HSM
- 审计链路
- 客户资产隔离
- 侵害赔偿机制

Q12：芬兰是否允许提供 OTC 服务?

允许，只要属于 MiCA 第 2 类服务："执行订单"。

Q13：芬兰是否可以经营加密衍生品?

一般属于 MIFID 范畴。
（并非 CASP 范围 → 需单独申请投资公司牌照）

Q14：芬兰是否监管 NFT?

若 NFT "金融化" → 属于 MiCA 投资代币类别。
若单纯艺术品 → 不属于 MiCA。

Q15：谁适合申请芬兰 CASP?

- Web3 企业
- DeFi 项目
- 加密钱包
- OTC 团队
- RWA 发行项目
- 交易所
- 托管机构

Q16：芬兰 MiCA 的优势是什么?

- 北欧监管信用极高
- 消费者保护体系成熟
- 稳定的政府与监管环境
- 优秀的银行体系（易开立账户）
- 可护照 30 国

Q17：获得芬兰 CASP 是否有利于全球融资?

是的，北欧牌照在 VC 中认可度高。
特别是对于 RWA、钱包、清算方向。

Q18：申请难度如何?

难度属于 **中偏高**。
难点在：

- AML
- 钱包安全
- 银行账户
- 实体要求

Q19：是否需要资本金?

MiCA 没有固定资本金要求，但：

- 托管类
- 交易平台类
  FIN-FSA 会要求更高的资本"证明资金"。

Q20：芬兰审查最严格的部分是什么?

- AML/CTF
- IT 安全（北欧强项）
- 客户资产隔离
- 客户保护
- 市场滥用防范

Q21：可否用非欧盟公司的高管?

可，但必须有至少 1 名芬兰本地关键人员。

Q22：是否可以使用外包 AML?

部分可外包，但 MLRO 不可外包。

Q23：是否需要提供审计报告?

托管类和平台类 → 必须年度审计。

Q24：监管是否要求提交内部政策文件?

必须提交至少 20 份 MiCA 政策（仁港永胜提供全套模板包）。

Q25：芬兰是否需要 IT 架构文件?

必须提交：

- 系统架构图
- 数据流图
- 加密方案
- Key Ceremony 文档

Q26：是否可以接受来自高风险国家客户?

必须执行高风险 EDD，某些国别需直接拒绝。

Q27：是否允许使用非欧盟云服务?

不建议。
数据最好存放在欧盟区域（强烈建议 AWS EU 或 Azure EU）。

Q28：是否可以使用智能合约进行托管?

可以，但必须提供代码审计报告（Smart Contract Audit）。

Q29：申请时是否必须已经运营？

不需要，但需提供：

- MVP
- IT 系统截图
- 测试环境

Q30：是否需要提交风险矩阵（Risk Matrix）？

是的，MiCA 要求必备材料。

Q31：FIN-FSA 是否会实地审查办公室？

有可能进行现场检查（On-site Inspection）。

Q32：是否需公布负责人信息？

关键人员（董事、MLRO）需在 FIN-FSA 名册公开。

Q33：是否允许 DeFi 与链上业务？

允许，但必须：

- 提供风险披露
- 说明智能合约的攻击风险
- 提供链上监控机制

Q34：是否需要合规手册？

必须提交完整 Compliance Manual。

Q35：是否允许跨国团队（香港 + 芬兰）共同运营？

可以，但实质管理层必须在芬兰。

Q36：是否对广告有特别限制？

禁止误导性广告，必须附加风险警告。

Q37：是否需提供客户保护机制？

必须，包括：

- 投诉流程
- 补偿机制
- 客户教育内容

Q38：WHOIS 信息是否包含在审查中？

FIN-FSA 可能会检查域名持有人信息。

Q39：申请能否加急？

不能加急，但资料完整可显著缩短时间。

Q40：申请成功率多少？

若文件齐全、团队专业：
成功率 85% 以上（由仁港永胜完整递件案例统计）

第二章｜申请流程、时间、监管问答（Q41～Q90）

Q41：申请芬兰 CASP 的完整流程是什么？

标准流程（FIN-FSA 官方 + 仁港永胜实操版本）：

1. **前期结构设计（2～4 周）**
   - 选择实体类型（Oy / Branch）
   - 设计治理结构
   - 选择业务类别（8 类 MiCA 服务）
   - 评估资金来源、股东背景
2. **文件准备阶段（6～10 周）**
   必备材料约 40～60 份，包括：
   - 商业计划书（BP）
   - 组织结构图
   - AML/KYC/CTF 政策
   - IT 架构资料
   - 风险管理框架
   - 客户资产隔离模型
   - 数据保护制度（GDPR）
   - 外包/技术服务文件
     （仁港永胜提供全套模板包）
3. **正式申报 FIN-FSA（2～4 天）**
4. **第一次补件 RFI（4～8 周）**
5. **第二次补件 RFI（可选，2～6 周）**
6. **FIN-FSA 审批（3～6 个月）**

Q42：申请芬兰 CASP 通常需要多久？

正常申请：6～10 个月
（含文件准备 + 审批）
复杂业务（平台运营/托管类）：9～14 个月

Q43：文件是否越多越容易获批？

不是。
FIN-FSA 强调"质量＞数量"，缺乏一致性反而被要求重写。
仁港永胜递件全部采用 **"结构化合规文件体系"**，确保逻辑一致。

Q44：FIN-FSA 最在意的文件是哪几份？

排名如下：

1. **AML/KYC/CTF Manual**
2. **IT 与信息安全政策**

3. **客户资产隔离体系（Safeguarding Model）**
4. **风险管理框架**
5. **董事、MLRO、管理层尽职调查文件**

Q45：申报人是否需要亲自去芬兰面谈？

绝大多数情况 **需要**。
FIN-FSA 会组织线上或线下面谈（1–2 小时）。
常见议题包括：

- 业务模型
- 客户旅程
- AML 场景
- 系统稳定性
- 风险管理

仁港永胜可准备 **面谈模拟问答（Mock Interview）**。

Q46：FIN-FSA 面谈通常问什么？

核心 5 类问题：
① **治理结构是否真实存在？**
② **AML 场景是否真实运行？**
③ **系统是否能审计？可否提供访问？**
④ **客户资产隔离是否真实做到？**
⑤ **是否有足够本地管理能力？**

Q47：是否可以先递交部分文件，后补充？

可以，但会触发 RFI，整体时间更长。
建议一次性提交完整、合规的材料。

Q48：是否可以边运营、边申请？

在 MiCA 环境下：
未获授权不得在芬兰"对外公开运营"。
但可在封闭测试环境下运行（Sandbox）。

Q49：申请 CASP 是否必须要银行账户？

强烈建议先开立：

- 欧盟 IBAN
- 企业运营账户
- 客户资产隔离账户（适用时）

如果没有银行账户，FIN-FSA 会怀疑业务可行性。

Q50：外国团队可否申请芬兰 CASP？

可以，但必须满足：

- 本地董事
- 本地 MLRO
- 本地办公室
- 本地审计师

Q51：申请人是否必须提供资金来源文件？

必须。
FIN-FSA 会要求：

- 资金来源证明（SOF）
- 资金合法性证明（SOL）
- 银行流水
- 投资协议（如适用）

Q52：是否可以用香港公司作为股东？

可以，但必须提供：

- 公司注册证书
- 组织章程
- 股东结构图
- UBO 声明
- 财务报表
- 层层穿透文件

仁港永胜可协助整理穿透结构包。

Q53：流程中 FIN-FSA 会与申请人保持多少次沟通？

通常包括：

1. 受理确认
2. 第一次 RFI
3. 第二次 RFI（如需要）
4. 授权会议
5. 面谈确认
6. 牌照下发通知

Q54：在 FIN-FSA 系统中提交申请需要多长时间？

提交本身只需要 **1～2 天**。
前期文件准备时间较长。

Q55：RFI（监管补件）通常多少题？

平均：

- **托管类、平台类：60～120 题**
- **其他类别：20～60 题**

Q56：RFI 会不会问技术细节？

会。
包括：

- 交易链路
- API 架构
- 钱包密钥管理

- MPC/多签方案
- 数据加密
- IT 日志保存

北欧对 IT 标准要求极高。

Q57：RFI 是否会要求录制 Demo?

非常常见。
需要提供：

- 系统操作流程
- KYC 流程
- 交易流程
- 风控触发场景
- 钱包操作演示

仁港永胜可协助准备完整 Demo 文档。

Q58：申请过程中能否更换董事或 MLRO?

可以，但必须重新提交：

- Fit & Proper 文件
- 尽职调查（CDD）
- 解释说明

若在 RFI 阶段更换，会延长审核时间。

Q59：申请 CASP 是否需要聘请本地律师?

建议聘请。
FIN-FSA 偏好看到：

- 本地法律顾问
- 本地会计师
- 本地审计师
- 本地办公室

仁港永胜通常为客户协调律师 + 会计师团队。

Q60：提交申请后是否可以修改商业计划?

可以，但必须提供：

- 更新说明
- 影响评估
- 修订版商业计划书（BP）

Q61：FIN-FSA 是否要求"关键职能不外包"?

是的，例如：

- AML/CTF
- 合规（Compliance）
- 风险管理（Risk Function）
- 客户资产隔离控制

这些都不能 100% 外包。

Q62：系统外包商是否必须在欧盟？

不强制，但强烈建议。
如果供应商数据中心在欧盟以外，必须提供 DPA + 数据保护机制。

Q63：申请时是否必须提交测试账户？

FIN-FSA 经常要求：

- Test Account
- System Access
- 测试环境链接

（仁港永胜可协助准备测试账号配置）

Q64：申请过程中若业务计划更改，会不会重审？

若属于重大变动（如新增服务类别）→ 必须重新评估。
若为轻微调整 → 可补充说明。

Q65：申请失败后是否可以重新申请？

可以，但必须提供：

- 改善说明
- 合规整改报告

Q66：FIN-FSA 是否会检查 UBO 的背景？

100% 会检查。
包括：

- 犯罪记录
- 金融背景
- 税务记录
- 资金来源
- 制裁名单筛查

Q67：申请过程中能否保持匿名股东？

不行。
MiCA 强制 UBO 完全透明。

Q68：董事是否必须全职？

至少 1 名董事需被视为"积极参与管理（Active Management）"。
不能是纯粹挂名。

Q69：申请中是否必须提交"客户投诉政策"？

必须。
北欧消费者保护文化非常严格。

Q70：申请是否需要提交"市场滥用政策（Market Abuse Policy）"?

是的，MiCA 新要求 CASP 必须有此文件。

Q71：申请是否必须提交 GDPR 政策?

必须，因为芬兰属于欧盟并严格执行 GDPR。

Q72：FIN-FSA 是否要求 stress test（压力测试）?

平台类、托管类企业 → 经常要求。

Q73：申请 CASP 时是否必须提供保险?

非强制，但 FIN-FSA 可能会建议：

- 专业责任险（PII）
- 网络安全保险

Q74：FIN-FSA 审查过程中是否会检查"三道防线"机制?

会检查：

1. 一线运营
2. 二线合规/风险
3. 三线内部审计

Q75：提交申请后是否可以立刻开始营销?

不行。
未获授权不得对外公开宣传 CASP 服务。

Q76：配套文件大约有多少页?

完整 MiCA 档案约：
600～1,200 页
（仁港永胜标准文件包）

Q77：是否需要双语文件（英语 + 芬兰语）?

FIN-FSA 接受英文。
不强制芬兰语。

Q78：FIN-FSA 是否会对系统进行安全扫描?

不会主动扫描，但会要求：

- 第三方渗透测试报告
- 漏洞扫描报告
- 代码审计报告（如托管/智能合约）

Q79：FIN-FSA 是否会要求 AML 系统访问?

经常会要求演示：

- 风险分层
- 客户画像
- 交易监控
- STR 提交流程

Q80：申请 CASP 是否有 Sandbox?

芬兰有 Sandbox 项目，但 MiCA 类别通常要求正式授权，而非沙盒许可。

Q81：是否可以"同时"申请多个 MiCA 类别?

可以，但：
业务越复杂，审查越严格。

Q82：审查过程是否允许提交追加材料?

允许。
FIN-FSA 鼓励提供有助于审查的补充文档。

Q83：FIN-FSA 是否接受 tokenomics 资料?

若涉及：

- 产品代币
- 平台代币
- 股权代币
- 稳定币
  必须提供白皮书 + 合规披露。

Q84：若使用 on-chain 数据分析工具（如 Chainalysis），是否加分?

加分。
北欧普遍认可链上分析服务。

Q85：是否允许使用多名 MLRO?

只允许 1 名 MLRO，可配置 Deputy（副 MLRO）。

Q86：FIN-FSA 是否要求提交全套内审计划?

年度内审计划需要提供，尤其平台类/托管类。

Q87：是否必须提供 Outsourcing Register（外包登记册）?

必须，MiCA 明确要求。

Q88：是否需要提供 Board Minutes（董事会议记录）?

申请阶段不强制，但部分审查可能要求。

Q89：FIN-FSA 是否会要求"退出计划（Exit Plan）"?

是 MiCA 强制要求，必须提交。

Q90：申请完成后多久能收到纸质牌照?

授权通过后 **1～2 周** 内可收到 FIN-FSA 正式授权文件（电子版）
纸本可申请邮寄。

第三章｜实体设立、治理架构、人员要求（Q91～Q150）

Q91：申请芬兰 CASP 必须使用什么法律实体?

可使用：

1. **芬兰有限公司（Oy）** → 最常用
2. **在芬兰设立分公司（Branch）** → 较少使用
3. **其他欧盟 CASP 的跨境护照（Passporting）** → 需已获他国 MiCA 授权

大多数申请人会新设 **Oy**，监管更偏好独立法人结构。

Q92：选择 “Oy” 与 “Branch” 的差别是什么?

选项	优点	缺点
Oy（子公司）	独立法律实体、监管更认可、易安排本地治理	成本更高
Branch（分公司）	成本低、快速设立	治理难满足 MiCA，监管更谨慎

FIN-FSA 90% 以上的 CASP 都使用 Oy。

Q93：芬兰 CASP 是否需要本地办公地址?

必须。
FIN-FSA 会核实：

- 真实办公地点
- 员工是否实际在当地工作
- 是否存在“纸面办公（Letter-box）”情形

虚拟办公室不被接受。

Q94：实体是否可以完全外包，没有本地员工?

不可以。
MiCA 要求：

1. AML 必须本地
2. 关键管理人员必须在芬兰
3. 实质性运营不能外包

Q95：董事会（Board）最低结构要求是什么?

通常要求：

- **至少 2 名董事（Board Members）**
- 其中 **至少 1 名为芬兰/欧盟本地居民**
- 董事必须具备金融与风险管理经验

Q96：董事是否需要具备加密行业经验?

不是强制，但有加分。
FIN-FSA 最看重：

- 金融行业经验
- 风险管理背景
- 法律/合规经验

Q97：董事必须长期居住在芬兰吗？

至少 1 名核心董事（Executive Director）必须：

- 常驻芬兰
- 全职履行管理职责
- 可现场接受监管问询

Q98：是否必须设立 CEO？

是的，芬兰 Oy 必须设 CEO（Managing Director）。
CEO 必须具备：

- 运营经验
- 风险管理经验
- 无犯罪记录

Q99：CEO 可以是外籍人士吗？

可以，但必须提供：

- 工作许可
- 税务登记
- 在芬兰本地实体任职证明
- Fit & Proper 文件

Q100：是否允许同一人担任 CEO + MLRO？

不允许。
MiCA 要求"职责分离"。

Q101：人员最低要求有哪几类？

共 6 大类关键人员：

1. 董事会成员（Board）
2. CEO（Managing Director）
3. 合规负责人（Compliance Officer）
4. 反洗钱负责人 MLRO
5. 风险管理负责人（Risk Officer）
6. 内部审计（Internal Audit）

Q102：董事会与执行管理层是否可以重叠？

部分重叠允许，但必须保持治理独立性，例如：

- CEO 不能同时担任董事会主席

- MLRO 不能同时管理一线业务

Q103：MLRO 是否必须在芬兰?

必须。
FIN-FSA 对 AML 的要求极高，必须确保：

- MLRO 本地实际办公
- 熟悉芬兰 AML Act
- 能与监管实时沟通

Q104：MLRO 必须具备哪些资质?

必须具备：

- 3–5 年以上 AML 实操经验
- 涉加密资产 AML 更佳
- 了解芬兰 AML Act + EU AMLD
- 可以附上培训证书（ACAMS 加分）

Q105：是否允许配置 Deputy MLRO（副 MLRO）?

允许且建议配置，以确保：

- 业务连续性
- 减少监管担忧
- 加强 AML 体系稳定性

Q106：风险管理负责人（Risk Officer）必须独立吗?

是的。
该角色不能兼任：

- CEO
- MLRO
- CFO
- 前台业务（Trading / Brokerage）

Q107：是否可以聘请外包公司担任内部审计（Internal Audit）?

可以。
FIN-FSA 接受：

- 本地会计事务所
- 审计服务机构
- 律师事务所团队

仁港永胜可协调芬兰本地审计团队。

Q108：是否必须配置数据保护官（DPO）?

建议配置，尤其是涉及：

- 欧盟客户数据
- 跨境数据传输
- 大量用户身份信息

GDPR 是北欧监管的重要考核点。

Q109：高管与关键岗位是否要通过 Fit & Proper 审查?

必须，包括：

- 犯罪记录
- 破产记录
- 税务记录
- 教育背景
- 专业资格
- 金融行业经验
- 过去执照情况

Q110：FIN-FSA 是否会对人员进行背景背调?

一定会。
并会要求提供：

- 犯罪记录证明（Police Certificate）
- 信用记录说明
- 税务证明
- 声明函

Q111：股东是否也需要 Fit & Proper?

需要，适用对象包括：

- 10% 以上股东
- 控制性股东（50% 以上）
- 公司股东的 UBO
- 公司股东的董事

Q112：股东是否必须为自然人?

不必须。
可以为：

- 香港公司
- 新加坡公司
- 欧盟公司
- BVI / Cayman（会加强审查）

Q113：是否可以使用多层控股结构?

可以，但必须满足：

- 结构透明
- 每一层提供证照
- UBO 完全穿透
- 无匿名信托结构
- 无壳公司隐藏股东

仁港永胜可协助制作穿透结构图（含控制关系解释信）。

Q114：股东是否必须提供银行流水？

MiCA 要求资金来源透明，因此通常需要提供：

- 6–12 个月银行流水
- 资产证明
- 投资金来源（SOF）
- 合法性证明（SOL）

Q115：若股东是公司是否必须提交审计报告？

通常要求提交最近 **1～3 年经审计财报**。
若无财报 → 必须提供资产负债声明 + 董事声明。

Q116：是否允许 100% 外国持股？

允许。
芬兰欢迎外资，不限制外国企业控股 CASP。

Q117：是否允许股票代持（Nominee）？

不允许。
UBO 必须完全透明。

Q118：是否必须聘请本地会计师？

必须。
目的包括：

- 税务申报
- 年度审计
- 监管报告

Q119：是否必须聘请本地法律顾问？

强烈建议。
FIN-FSA 通常希望看到专业法律意见。
仁港永胜提供"合规＋法律"双轨团队。

Q120：是否必须设立合规委员会（Compliance Committee）？

非强制，但平台类公司通常会设立，有利于：

- 董事会监管
- 合规优先机制
- 高级管理层责任分配

Q121：Trust、基金、家族办公室是否能作为股东？

可以，但必须满足：

- 完整穿透
- 提供信托契约
- 提供受托人信息

- 提供基金管理人信息
- 提供最终受益人资料

Q122：是否必须提供公司组织章程（Articles of Association）？

必须。

Q123：董事会会议需要多久召开一次？

建议：

- **每季度至少一次**
- 重大事项可召开临时会议

必须有会议记录。

Q124：董事会会议记录是否必须提交给 FIN-FSA？

申请过程中通常不需要，但审查时可能要求。
授权之后 → FIN-FSA 有权随时要求提供。

Q125：是否必须有薪资发放？

必须。
FIN-FSA 不接受"0 员工 + 挂名岗位"的情况。

Q126：能否使用兼职人员？

部分岗位允许兼职，但以下岗位不允许：

- CEO
- MLRO
- Risk Officer

Q127：是否需要设立本地 HR？

不是强制，但对于大型 CASP（如平台类）有加分。

Q128：是否必须设立 CFO？

非强制，但建议设立，尤其涉及：

- 客户资产隔离
- 大额资金管理
- 稳定币相关业务

Q129：是否可以让董事兼任 CFO？

小型 CASP 可以，但不建议，因为：

- CFO 需参与风险管理
- 董事职责可能冲突

Q130：是否可以让 CEO 兼董事？

可以，但 CEO 不能兼任董事会主席。

Q131：是否必须有实际办公桌？

需要。
FIN-FSA 对"Letter-box 实体"非常警惕。

Q132：是否允许在芬兰没有运营人员，远程办公？

不允许。
关键岗位必须在芬兰办公。

Q133：是否必须在芬兰缴纳税？

是的。
Oy 属于芬兰本地纳税实体，需要缴纳：

- 企业所得税（20%）
- 增值税（如适用）
- 本地员工税

Q134：股东是否需要缴税？

非芬兰居民股东仅对芬兰来源的收入缴税。

Q135：董事是否需要个人纳税号？

需要。
必须办理芬兰税务号（Tax ID）。

Q136：是否可以设立有限合伙企业申请 CASP？

不可以。
必须为 **Oy（股份有限公司）**。

Q137：实体名称是否有限制？

禁用：

- Bank / Banking / Credit
- Exchange（部分情况）
- Official
- Regulated
- Finland Government

建议名称：
"XXX Digital Asset Services Oy"

Q138：是否会检查董事过去失败的企业？

会。
但不是一票否决，关键是是否有：

- 欺诈
- 逃税
- 金融许可证被吊销

- 监管处罚

Q139：董事是否需要提供当地地址证明?

需要提交：

- 租房合同
- 水电账单
- 税务文件
- 注册地址证明

Q140：管理层是否有最低学历要求?

没有明确规定，但一般期望：

- 本科或以上
- 金融/法律/会计专业加分

Q141：是否可以让外包公司担任 MLRO?

不可以。
AML 必须内部人员承担。

Q142：内审是否可以一年执行一次?

可以，但大型 CASP 建议半年一次。

Q143：是否必须聘请外部审计?

必须聘请注册会计师（CPA）进行年度审计。

Q144：董事会中需要女性成员吗?

非强制，但芬兰提倡性别平衡，有加分。

Q145：是否允许董事为无偿任职?

不建议。监管可能怀疑真实性。

Q146：是否需要设立薪酬政策（Remuneration Policy）?

MiCA 要求必须有：

- 薪酬结构
- 激励制度
- 风险限制机制

Q147：是否需要提交人员培训计划?

必须，包括：

- AML 培训
- 风险培训
- 系统安全培训

- GDPR 培训

Q148：是否可以聘请非芬兰籍 MLRO?

可以，但必须：

- 有工作许可
- 有芬兰本地实际办公
- 有 AML 实操经验

Q149：是否必须设立运营部门（Operations）？

平台类、托管类必须。
经纪类（Brokerage）通常也需要。

Q150：管理层必须懂编程吗?

不是硬性要求，但平台类 CASP 需具备较强的技术理解能力。

第四章｜AML / KYC / 客户保护 / 风险管理

（覆盖 FIN-FSA 最重视的部分，亦是 MiCA 合规核心）

Q151：芬兰 CASP 申请中 AML（反洗钱）是最重要的考核项吗?

是。
FIN-FSA 对 AML 的重视程度 **高于所有其他项目**，甚至高于业务模型。
监管主要关注：

1. 识别客户能力（KYC）
2. 交易监控能力（Monitoring）
3. 风险分层模型（Risk Scoring）
4. STR 可疑交易报告流程
5. 钱包监控能力（On-chain AML）
6. MLRO 的能力与实际参与度

Q152：AML 手册必须达到什么深度?

至少包括 **15 大章、150+ 页** 的完整 MiCA AML Framework：

- 客户尽职调查（CDD/KYC）
- 增强尽职调查（EDD）
- 政治公众人物（PEP）机制
- 制裁筛查
- 交易监控
- STR 报告
- 钱包监控（Chainalysis/Merkle Science）
- 黑名单管理
- 风险控制矩阵（RCM）
- 员工培训模块
- 审计与复核流程

仁港永胜提供"监管认可版 AML 手册"，可直接用于 FIN-FSA 递件。

Q153：是否允许将 AML 工作外包?

MiCA 明确禁止：

- AML 不可外包
- CDD/KYC 不可外包全部工作
- 核心 AML 决策必须由 MLRO 作出

可外包的部分包括：

- 第三方验证工具（OCR / Video KYC）
- 链上分析服务
- 名单筛查服务（PEP & Sanctions）

Q154：KYC 最低审查要求是什么?

必须包括：

1. 身份文件（护照/ID）
2. 活体检测（Liveness）
3. 地址证明（3 个月内）
4. 银行卡或账户验证
5. 是否为 PEP
6. 是否列入制裁名单
7. 资金来源说明（如适用）

Q155：是否必须提供 Enhanced Due Diligence（EDD）流程?

必须。
适用场景包括：

- 高风险国家
- 高净值客户
- OTC 大额购买
- 商业账户
- 涉虚拟资产混币器
- 技术匿名工具（TOR）
- 存在风险警示（Red Flags）

Q156：是否必须进行"地址验证"?

必须。
监管常要求提供：

- 水电账单
- 银行账单
- 政府文件
- 手机账单（部分接受）

Q157：是否必须对 crypto-to-crypto 交易进行 KYC?

必须。MiCA 强制：

- **所有客户均需 KYC**
- 不存在 "仅加密资产交易免 KYC" 这种情形

Q158：是否必须收集资金来源（SOF）与财富来源（SOW）？

部分客户必须收集：

- 高风险客户
- 大额交易客户
- 触发风险警报的客户

Q159：是否必须配置交易监控系统?

必须。
FIN-FSA 会检查系统是否能处理：

- 异常行为监控
- 暗网相关地址识别
- 新地址风险评分
- 机器学习模式（如可用）

Q160：是否必须有链上监控工具?

必须具备至少一种：

- **Chainalysis**
- **Elliptic**
- **Merkle Science**
- **Scorechain**

Q161：是否允许用自建链上监控系统?

允许，但必须提供：

- 技术说明
- 风险模型
- 准确度说明
- 演示视频

Q162：STR（可疑交易报告）多久内提交?

芬兰要求：
"without undue delay"
通常等同于：**24～48 小时内**。

Q163：STR 是否必须提交给芬兰金融情报部门（FIU）？

是。
并且必须有独立渠道 + 内部记录。

Q164：是否必须设立"交易阈值"机制?

必须。
典型阈值包括：

- 24 小时累计
- 一周累计

- 大额一次性交易
- 连续、多次小额交易（Structuring）
- 快速进出金

Q165：风险分层模型（Risk Scoring Model）必须包括哪些参数?

至少包含 10 类：

1. 地区风险
2. 客户类型风险
3. 交易类型
4. 交易频率
5. 金额级别
6. 链上地址风险
7. 产品类型（平台/经纪/托管）
8. 行为模式风险
9. KYC 完整性
10. 外部负面信息（Adverse Media）

Q166：是否必须检查客户的"负面新闻"（Adverse Media Screening）?

必须。

Q167：是否必须建立"客户适当性评估"机制?

MiCA 新要求：

- 投资匹配度
- 风险承受能力
- 客户分类（Retail / Professional）

Q168：是否需要配置"市场操纵检测机制"?

MiCA 强制要求平台类（Trading Platform）提供：

- 洗售交易（Wash Trading）
- 拉升出货
- 价格操纵
- 虚假买卖盘（Spoofing）

Q169：是否必须设立"客户资产隔离"机制?

必须。MiCA 明确要求：

- 客户资产与公司资产必须完全隔离
- 必须有专属账户（Safeguarding Account）
- 不得挪用客户资产

Q170：客户资产是否必须存在芬兰本地银行?

不是强制，但建议。
允许：

- 欧盟银行
- 欧盟电子货币机构（EMI）
- 欧盟托管合规机构

Q171：平台是否必须提供"冷钱包"机制?

托管类 CASP 必须具备：

- 冷钱包
- 多签/MPC
- 分层权限
- 私钥管理流程

Q172：是否必须披露"私钥管理方案"?

FIN-FSA 要求提供：

- 私钥生成流程
- 备份方式
- 使用方式
- 谁掌握权限
- 多签方案
- 灾难恢复（DRP）

Q173：是否必须提供"渗透测试报告"?

是的，托管类和平台类必须提交：

- 年度 PEN Test 报告
- 漏洞扫描报告

Q174：是否必须提交"IT 安全政策（IS Policy）"?

必须。内容包括：

- 身份验证机制
- 访问控制
- 数据加密
- 密码规则
- 操作日志（Audit Log）
- 云服务管理
- 灾备机制

Q175：是否必须提供"Incident Reporting Framework"?

必须。
MiCA 要求：

- 收集
- 分级
- 通知
- 升级
- 修复

- 复盘

Q176：系统数据是否需保存 5 年？

是的。
MiCA 要求至少 **5 年完整记录**。

Q177：是否必须配置"网络安全保险"？

非强制，但能加分：

- 网络攻击保险
- 客户资产保护保险（如适用）

Q178：是否必须提供"用户协议（Terms & Conditions）"？

必须。
内容包括：

- 费用透明度
- 风险披露
- 资产管理方式
- 客户资产隔离
- 投诉机制
- 退款政策

Q179：是否必须提供"风险披露声明（Risk Disclosure Statement）"？

必须。
尤其针对散户客户。

Q180：是否必须检查客户是否为未成年人？

必须验证年龄 ≥18 岁。

Q181：是否可以允许匿名交易？

完全禁止。
所有客户必须完成 KYC。

Q182：是否可以允许客户使用隐私币？

FIN-FSA 对隐私币态度谨慎：

- 若允许 → 必须 100% 证明可监控
- 若无法监控 → 不允许提供此服务

Q183：是否必须配置"客户投诉程序"？

必须，MiCA 要求：

- 投诉处理流程
- 解决时间
- 升级流程

- 文档留存

Q184：投诉处理需多久完成?

MiCA 要求：

- **15 天内回复客户**
- **8 周内必须解决**

Q185：是否可以让 MLRO 兼任合规负责人（Compliance Officer）?

不允许。

Q186：是否必须进行员工的年度 AML 培训?

必须，并需记录：

- 参加者
- 培训内容
- 测试结果
- 培训记录保存 5 年

Q187：系统是否必须支持"黑名单地址阻拦"?

必须。
包括：

- OFAC
- 欧盟制裁名单
- 私有黑名单
- 高风险链上地址

Q188：是否必须提供"钱包白名单机制"?

托管类 CASP 强烈建议提供。

Q189：是否要对商业客户（Corporate Accounts）执行 EDD?

必须执行增强尽调：

- UBO 穿透
- 董事身份
- 财务状况
- 商业模式
- 反洗钱风险

Q190：是否需要审查商业客户的资金来源?

必须。

Q191：是否允许客户使用第三方钱包充值?

允许，但必须监控：

- 充值地址
- 链上风险
  -地址所有权（可证明）

Q192：是否允许高风险国家客户注册？

可注册，但必须执行：

- EDD 加强尽调
- 强化监控
- 高风险评分
- 定期复审

部分极端高风险国家必须拒绝。

Q193：是否必须设立"客户投资损失免责说明"？

MiCA 要求全面披露风险，但不能完全免责。

Q194：是否必须提供"业务连续性计划（BCP）"？

必须，包括：

- 系统故障
- 数据丢失
- 网络攻击
- 灾难恢复
- 人员变动

Q195：灾备中心必须在哪个国家？

建议设在：

- 芬兰
- 其他欧盟国家（同样接受）

Q196：系统是否必须提供双重验证（2FA）？

必须。

Q197：是否允许客户关闭 2FA？

不能关闭。
MiCA 要求严格安全标准。

Q198：是否必须提供活动日志（Activity Log）？

必须，并需保存 5 年。

Q199：是否必须提供 KYC 视频存档？

若使用 video KYC → 必须保存。

Q200：是否可以只做轻量版 AML？（例如仅身份证 + 地址）

不可能获批。
MiCA + FIN-FSA 要求全面 AML。

Q201：是否必须提供"跨境风险评估"文件?

必须提交，尤其：

- 客户来自哪些国家
- 风险等级
- 区域特征

Q202：是否需要提供"地缘政治风险评估"?

大型 CASP → 建议提供
小型 CASP → 可不提供，但 RFI 经常要求

Q203：是否需要提供冻结机制（Freeze Function）?

托管类必须。

Q204：是否需要"内部可疑名单（Internal Red-flag List）"?

必须。

Q205：员工是否需要每年重新接受 AML 考试?

建议强制执行。

Q206：是否需要检查员工背景（Staff Screening）?

必须提交：

- 犯罪记录
- 工作历史
- 身份验证

Q207：是否需要监控员工账号的系统操作?

必须。
FIN-FSA 会检查：

- 管理后台日志
- 权限分层
- KPIs
- 员工行为监控

Q208：是否必须提供"内部举报制度（Whistleblowing Policy）"?

必须，MiCA 明确要求。

Q209：AML 报告是否需要每年更新?

必须每年提交 AML 报告（Annual AML Report）给董事会。

Q210：FIN-FSA 是否会要求实际测试 AML 场景?

会。
例如：

- 测试 PEP 检测
- 测试链上风险识别
- 测试可疑交易上报
- 测试客户风险变更

第五章｜IT / 技术架构 / 数据保护 / 网络安全（Q211～Q280）

Q211：芬兰 CASP 申请中 IT 技术要求是否非常严格?

是的。
FIN-FSA 属于欧盟技术审查最严格的监管之一，与德国 BaFin 接近。
重点审查：

1. 系统安全性
2. 数据保护（GDPR）
3. 客户资产隔离技术
4. 钱包密钥管理
5. 访问权限控制
6. 审计日志
7. 事件/事故响应
8. 第三方外包风险

Q212：申请时是否必须提交完整 IT 架构图?

必须提供至少：

- 总体系统架构图（High-level Architecture）
- 交易链路架构
- 钱包架构（MPC/多签/冷钱包）
- API 架构
- 数据流图（Data Flow Diagram）
- 外包服务节点图（Outsourcing Architecture）

仁港永胜可提供欧盟监管版本架构图模板。

Q213：是否必须提供"数据流（Data Flow）"图?

必须。
FIN-FSA 强调：
"数据在哪、如何流动、从哪里出去"
必须完全透明。

Q214：是否需要记录系统所有操作日志?

必须，并且保存 **至少 5 年**。
包括：

- 登录日志

- 交易日志
- 钱包操作日志
- 员工后台操作日志
- 审计日志（Audit Trail）

Q215：是否必须使用多重身份验证（2FA/MFA）？

必须。
客户端 + 员工后台均须启用。

Q216：是否可以使用"邮箱 + 密码"作为唯一登录方式?

不允许。
必须至少：

- 密码 + 2FA（谷歌验证器/SMS）
- 或 FIDO2 生物识别方案

Q217：是否必须提供 API 安全机制?

必须，包括：

- API Token
- 访问权限分级
- 日志追踪
- 速率限制（Rate Limiting）
- 签名验证（HMAC）

Q218：是否必须执行年度渗透测试（PEN Test）？

必须，并提交：

- 第三方渗透测试报告
- 漏洞扫描报告
- 修复说明（Fixing Report）

Q219：是否需要提供云服务合规证明?

必须提交：

- 云服务协议
- 数据保护协议（DPA）
- 数据中心位置说明
- 安全措施（ISO27001、SOC2 等）

Q220：云服务必须在欧盟境内吗?

建议，但不是强制。
若使用：

- AWS
- Azure
- Google Cloud

必须确保数据节点在 **欧盟可选区（EU Region）**。

Q221：是否可以使用非欧盟云服务？

可以，但更严格：

- 必须提供跨境数据保护机制
- 必须提供 Data Export 影响评估（TIA）
- 必须遵守 GDPR

Q222：系统是否必须支持"灾难恢复（DRP）"？

必须，包括：

- 数据备份
- 节点恢复
- 故障切换（Failover）
- 恢复时间目标（RTO）
- 恢复点目标（RPO）

Q223：必须提供灾备环境（Secondary Environment）吗？

托管类、平台类必须。
经纪类可选择性提交。

Q224：客户数据是否必须加密存储？

必须遵守加密要求：

- AES-256
- TLS 1.2/1.3
- 敏感数据脱敏（Masking）

Q225：是否要求加密密钥管理流程？

必须。包括：

- 密钥生成程序
- 密钥存储方式（HSM/MPC）
- 轮换周期
- 访问权限
- 审计记录

Q226：钱包密钥（private key）必须使用 HSM 吗？

不是强制，但使用 HSM 可以增加获批概率。
FIN-FSA 接受：

- MPC
- 多签
- HSM
- 冷钱包

Q227：是否可以使用第三方托管钱包服务？

可以，但必须确保：

- 托管服务机构具备欧盟合规资格
- 提供 SLA
- 提供安全证明
- 提供渗透测试报告

Q228：是否必须提供冷钱包策略?

托管类 CASP 100% 必须提供。
包含：

- 冷/热钱包比例
- 多签方案
- 提币审批流程
- 风险管理
- 故障处理

Q229：是否允许"自托管"方案?

允许。
但 FIN-FSA 会要求演示安全控制：

- 密钥不泄露
- 权限分层
- 多人审批
- 不依赖单一点故障

Q230：是否允许"使用员工钱包"(如 MetaMask）管理客户资产?

完全禁止。
必须使用专业托管机制。

Q231：系统是否必须提供权限分层?

必须。
典型权限包括：

- 查看
- 操作
- 管理
- 审批
- 提币
- 财务
- 风控
- 系统配置

Q232：是否必须提供 RBAC（基于角色的访问控制）?

必须。

Q233：是否必须提交权限矩阵（Access Matrix）?

FIN-FSA 通常要求提交 40～80 项权限矩阵。

Q234：系统是否必须支持"职能分离（Segregation of Duties）"?

必须确保：

- 前台 / 中台 / 后台 分离
- 操作 / 审批 分离
- 提币 / 审批 分离

Q235：是否需要提交内部控制（Internal Control）文件?

必须。
包括：

- 控制流程
- 审计流程
- 风险矩阵

Q236：是否需要提供数据保留机制?

必须：

- 数据保存 ≥5 年
- 数据可随时导出
- 提供加密存储证明

Q237：是否要求"禁止删除日志"?

是的。
所有活动必须可审计：

- 禁止删除
- 禁止覆盖
- 禁止隐藏

Q238：是否需要提供操作手册（SOP）?

必须，尤其是：

- 入金
- 出金
- 交易
- 提币审批
- 钱包操作流程

Q239：是否必须有系统监控（System Monitoring）?

必须包括：

- CPU、内存监控
- 交易流量监控
- 故障报警（Alert System）
- SLA 报告

Q240：是否必须提供"事件响应计划（Incident Response Plan）"?

必须，包括：

- 事故识别
- 分级
- 通知
- 修复
- 复盘与改进

Q241：系统是否必须支持"异常行为检测"？

平台类必须具备，如：

- 多次失败登录
- 异常频率操作
- 可疑 IP
- 异常交易模式

Q242：是否必须提供安全开发流程（Secure SDLC）？

必须，包括：

- 开发阶段审查
- 代码审计
- 上线前测试
- 变更记录（Change Log）

Q243：是否必须提供代码审计报告？

托管类 / 交易平台类必须。
经纪类可选。

Q244：是否必须使用 MFA 保护管理员账户？

必须。

Q245：是否必须提供防火墙（Firewall）配置？

必须提供：

- 防火墙架构
- 安全规则
- 访问控制

Q246：必须提供 DDoS 防护吗？

平台类、托管类 → 必须
经纪类 → 建议

Q247：客户数据是否可以存储在芬兰以外的国家？

允许，但须满足：

- GDPR
- EU 数据出口条款

- 跨境传输影响评估（TIA）

Q248：必须提供 GDPR 文件吗?

必须提供至少：

- GDPR 政策
- 数据主体权利流程
- 数据泄露通知机制
- 数据处理协议（DPA）

Q249：系统是否必须具备加密传输（TLS）？

必须。

Q250：是否必须提供备份加密方案?

必须：

- 加密备份
- 地理隔离备份
- 定期恢复测试

Q251：是否必须提交"第三方供应商清单（Vendor Register）"?

必须。
MiCA 要求透明披露所有外包关系。

Q252：是否必须对外包商进行尽职调查?

必须，包括：

- 安全审查
- 合规证明
- 业务持续性
- 合同管理

Q253：是否可以使用离岸外包公司?

可以，但需提供：

- 控制机制
- 安全措施
- 数据保护协议

监管会更谨慎。

Q254：是否必须提交外包政策（Outsourcing Policy）？

必须，MiCA 对外包管理要求严格。

Q255：系统是否必须实时可审计?

必须，要求：

- 全链路日志
- 审计接口
- 管理后台可追踪

Q256：是否必须提供"系统 demo 视频"?

FIN-FSA 常要求，特别是：

- KYC 流程
- 钱包操作
- 风险监控
- 交易流程

仁港永胜可协助制作正式监管版 Demo。

Q257：是否必须提供"管理员权限演示"?

通常要求：

- 提币审批
- 权限变更
- 钱包操作
- 风险警报处理

Q258：是否须提交"合规监控系统"架构?

必须，包括：

- AML Monitoring
- 行为监控
- 市场操纵检测

Q259：是否需要提交"监控警报处理流程（Alert Handling）"?

必须，包含：

- 警报分类
- 响应时间
- 处理流程
- 记录机制

Q260：是否必须设置"关键事件自动告警"?

平台类、托管类必须：

- 错误交易
- 钱包异常
- 提币异常
- 系统中断

Q261：是否需要提供"系统访问历史"证明?

必须提交样例日志。

Q262：系统日志保存多久？

MiCA 要求 **≥5 年**。

Q263：是否必须有"隐私设计（Privacy by Design）"？

GDPR 要求必须遵守。

Q264：是否需要提交"变更管理流程（Change Management）"？

必须，包括变更：

- 提交
- 审批
- 实施
- 回滚
- 文档记录

Q265：是否要提供"发布管理（Release Management）"文档？

经常要求。

Q266：是否需要提供"自动化测试机制（Automated Testing）"？

平台类建议提供。

Q267：系统必须支持"可审计性（Auditability）"？

是 MiCA 核心要求之一。

Q268：是否必须提交"系统稳定性报告（System Stability Report）"？

大型 CASP 常被要求。

Q269：必须提供"服务等级协议（SLA）"吗？

外包商必须提供 SLA。

Q270：是否要提交"负载测试（Load Test）"？

平台类必须。
经纪类、托管类 → 视情况决定。

Q271：是否必须提供"系统容量规划（Capacity Planning）"？

必须。监管要确保系统可持续运行。

Q272：是否需要提交"证据链管理（Chain of Evidence）"？

平台类 / 托管类通常被要求。

Q273：是否必须提供"故障报告（Incident Report）"样本？

FIN-FSA 经常要求申请人提交 Sample。

Q274：是否必须提供"IT 审计计划（IT Audit Plan）"?

建议提供，增加可信度。

Q275：必须提供"风险控制矩阵（IT RCM）"吗?

必须。

Q276：是否需要提交"数据泄露应对流程（Data Breach Procedure）"?

必须，包括：

- 发现
- 分级
- 通知（72 小时内）
- 修复
- 报备

Q277：是否要提供"信息分类政策（Information Classification Policy）"?

必须提交。

Q278：是否必须提供"IT Outsourcing Register"?

必须，是 MiCA 要求的一部分。

Q279：是否需要提交"系统可用性（Uptime）记录"?

平台类通常要求提供 3～6 个月数据。

Q280：FIN-FSA 是否会真正登录我们的系统查看?

会。
FIN-FSA 会要求：

- Test account
- Admin account（权限受控）
- 查看风险监控
- 查看交易流程
- 查看日志

仁港永胜可协助准备审查账户。

第六章｜业务模式、产品合规、托管、平台运营

（Q281～Q340）

Q281：芬兰 CASP 可以开展哪些业务?

MiCA 定义的 8 大服务全部可在芬兰获批：

1. **接收与传送订单（Order Reception & Transmission）**

2. **执行订单（Execution of Orders）**
3. **加密资产交易平台运营（Trading Platform Operation）**
4. **加密资产托管服务（Custody & Safekeeping）**
5. **资产管理（Portfolio Management）**
6. **投资建议（Investment Advice）**
7. **承销与发行（Crypto-Asset Offering & Placement）**
8. **交换服务（Crypto-Fiat / Crypto-Crypto）**

芬兰与德国、法国同属 **可申请全部 8 项 CASP 服务** 的国家。

Q282：是否可以只申请其中几个服务?

可以。
MiCA 允许申请：

- 单一服务
- 多服务组合
- 全服务组合（All-in CASP）

但服务越多，审查越严格。

Q283：什么业务最容易获批?

难度从低到高：

1. **经纪类（Brokerage / Exchange）**
2. **订单执行（Execution）**
3. **投资建议（Advice）**
4. **资产管理（Managed Portfolio）**
5. **托管（Custody）**
6. **平台类（Trading Platform）**

Q284：什么业务最难获批?

最难的三类：

1. **托管 Custody（私钥管理风险）**
2. **交易平台（完整市场风险）**
3. **自营交易／撮合引擎类业务**（涉及冲突风险）

Q285：CASP 牌照是否等同于加密交易所许可?

不完全等同。
MiCA 下，**交易平台（Trading Platform）** 是单独的授权类别。
如要运营交易所，必须申请：

- **第 3 类：Trading Platform Operation**
  ＋
- 其他增值服务（如托管、撮合）

Q286：是否允许运营"全牌照交易所"（全功能平台）？

允许，但监管难度极高：

- 需完整订单簿系统

- 深度市场监控
- 市场操纵检测机制
- 全套 IT 证明
- 冷热钱包分层托管
- 客户资产隔离模型
- 完整内部控制体系

Q287：平台类业务是否必须拥有做市商（Market Maker）？

不是强制，但监管会要求：

- 流动性方案
- 风险评估
- 做市商协议

Q288：是否必须提供订单簿模式（Order-book）？

若申请交易平台，监管要求：

- 订单簿系统
- 匹配引擎
- 成交撮合规则

Q289：是否允许 CEX + OTC 混合模式?

允许，但必须清晰划分：

- OTC 价格来源
- 平台订单簿机制
- 客户资金流向
- AML 风险隔离

Q290：是否允许 P2P 平台?

可以，但 FIN-FSA 会要求：

- AML 防范
- 平台只做撮合不托管
- 风险披露
- 场外转账监控

Q291：是否允许自动撮合引擎?

允许。
但需提交：

- 撮合规则
- 风险控制
- 风险提示
- 技术文档

Q292：是否允许类似"Robinhood"模式的零手续费交易?

允许，但必须披露：

- 隐性成本
- 订单流机制（PFOF – Payment for Order Flow）
- 利益冲突管理

Q293：芬兰是否允许运营 DEX 交易所?

监管态度：

- **DEX≠CASP**（无控制权则非 CASP）
- 若有控制权（前端、托管、订单簿、LP 机制）→ 必须申请 CASP
- 若无控制权 → FIN-FSA 不认为是 CASP，但需谨慎披露风险

Q294：是否允许提供代币发行（Token Offering）?

可以，但属于 MiCA 下的服务类别之一：

- Crypto-Asset Offering
- Placement
- Subscription Services

必须遵守：

- 白皮书披露
- 投资者保护
- 风险揭示

Q295：是否允许发行稳定币（EMT/ART）?

仅当：

- 申请独立的 **EMT/ART 发行许可证**（MiCA Title III / IV）
- 完整储备金机制
- 审计控制
- 客户赎回机制

CASP 本身 **不能** 自动发行稳定币。

Q296：是否允许自发行交易所平台币（Utility Token / Exchange Token）?

可以，但需要：

- 披露白皮书
- 风险说明
- 避免被认定为 ART/EMT
- 交易规则透明

监管重点看 **是否具有回购、收益、抵押特性**。

Q297：是否允许提供杠杆／衍生品交易?

MiCA 对衍生品和杠杆产品极为谨慎：

- 若为加密衍生品 → 属于 **MIFID II 金融工具**，可能需要 **欧盟投资公司牌照（Investment Firm License）**
- 不能通过 CASP 直接提供杠杆、永续合约

Q298：是否允许提供复制交易（Copy Trading）？

允许，但 FIN-FSA 会严格审查：

- 是否实质上构成投资建议
- 管理资产性质
- 风险披露
- 自动化触发机制

Q299：是否允许提供收益产品（Staking、Earn、Lending）？

MiCA 过渡期内仍允许，但必须满足：

- 非集体投资
- 非存款业务
- 非证券化产品
- 风险揭示充分

未来可能转为欧盟 CMU 法规监管（需持续关注）。

Q300：是否允许托管客户资金?

托管属于 MiCA 明确授权的 CASP 服务之一，但监管最严格。
必须提供：

- 冷/热钱包机制
- 多签 / MPC
- 密钥管理流程
- 提币审批机制
- 事故应急流程
- 客户资产隔离账户

Q301：托管业务需要哪些最低技术条件?

必须提供：

1. 资产分层（冷/热）
2. 储备金证明
3. 密钥管理文档
4. 签名机制
5. 内部权限控制
6. 访问审计
7. 事故恢复机制
8. 备份与冗余

Q302：托管私钥必须使用多签或 MPC 吗?

不是强制，但以下会大幅提高成功率：

- 多签
- MPC
- HSM

Q303：托管是否允许"第三方托管 + 自托管混合"?

允许，但必须保证：

- 透明的托管结构
- 风险分配
- 客户资产隔离
- 第三方资质

Q304：托管是否必须使用冷钱包？

托管类适用：

- 冷钱包比例通常要求 ≥70%
- 热钱包用于日常运营

Q305：私钥托管失败是否必须赔偿？

MiCA 要求托管方承担 **严格责任（Strict Liability）**。

Q306：是否允许"交易所内部子账户划转"？

允许，但必须：

- 保留日志
- 风险监控
- 资产隔离

Q307：是否允许"暗池交易（Dark Pool）"？

不允许。
MiCA 要求公开透明。

Q308：是否允许做市商与交易所为同一公司？

允许，但 FIN-FSA 会加强审查：

- 利益冲突管理
- 交易监控
- 做市商透明度

Q309：是否必须提交"市场操纵监控机制"？

交易所类业务必须。
包含：

- Wash Trading
- Spoofing
- Pump & Dump
- Cross Trading

Q310：是否必须提交"业务流程图（Process Flow）"？

必须，典型包括：

- 客户旅程
- 订单执行流程

- 出入金流程
- 托管流程
- 提币审批流程

Q311：是否必须披露"定价机制"?

必须，包括：

- 价格来源
- 手续费结构
- 点差（Spread）

Q312：是否允许在平台上提供第三方项目的白皮书?

允许，但需：

- 风险披露
- 白皮书审核
- 避免误导

Q313：是否允许"投资顾问 + 经纪"组合服务?

允许，但：

- 顾问必须保持中立
- 避免利益冲突
- 必须提供适当性评估

Q314：是否必须提交"利益冲突管理政策"（Conflicts of Interest）?

必须，内容包括：

- 自营交易披露
- 做市商利益关联
- 顾问与交易的分离
- 员工持仓规则

Q315：是否允许员工在平台交易?

可以，但需：

- 员工交易政策
- 披露
- 限制
- 黑名单机制

Q316：是否必须提供"营销合规（Marketing Compliance）"政策?

必须。
FIN-FSA 非常重视：

- 不得误导
- 风险披露
- 不得宣传收益

- 不得夸大安全性

Q317：是否允许跨境营销?

允许，但必须符合目标国法规。

Q318：MiCA 是否允许 CASP 代持客户代币?

允许，但必须强制隔离：

- 客户资产（Client Assets）
- 自有资产（Own Funds）

Q319：是否允许进行"token listing"（上币）服务?

允许，但需：

- 项目尽职调查
- 技术测试
- 风险分类
- 白皮书合规性确认

Q320：是否必须执行 Token Risk Assessment?

必须，包括：

- 技术风险
- 项目风险
- AML 风险
- 市场风险

Q321：是否允许提供"加密支付服务"?

若涉及：

- 商户收单
- 加密支付
- 结算

可能需要 **支付机构（PI）或电子货币（EMI）牌照**。

Q322：是否可以运营 OTC 业务?

可以，但 FIN-FSA 重点审查：

- 价格来源
- AML 风险
- 大额交易监控
- 商户客户审核

Q323：OTC 与平台交易是否需要分离?

必须分开：

- 流程

- 风险
- 资产
- 定价

Q324：OTC 是否可以不托管资产？

可以，只做经纪。

Q325：是否允许"客户间直接交易"功能？

可以，但平台不能干预定价。

Q326：是否必须提供"自动清算系统"机制？

平台类必须提供：

- 结算规则
- 清算流程
- DvP 机制（Delivery vs Payment）

Q327：是否允许"交易挖矿""手续费返还"类激励？

允许但必须：

- 风险披露
- 明确规则
- 避免误导
- 遵守市场公平原则

Q328：是否可以提供"预上市交易（Pre-listing Trading）"？

不建议。
FIN-FSA 认为风险极高。

Q329：是否可以运营 Launchpad？

可以，但必须：

- 白皮书合规
- 风险评估
- 投资者保护机制
- 不构成证券发行

Q330：是否可以运营 Earn/Staking 服务？

需要明确区分：

- 自营 vs 代操作
- 托管 vs 未托管
- 是否涉及证券化
- 投资风险披露

Q331：Staking 是否需要额外监管？

若涉及：

- 集体投资
- 预期收益
- 托管
  则可能被认定为其他欧盟金融工具。

Q332：是否允许自动机器人交易（Algo Trading）？

允许，但需：

- 风险控制
- 稳定性证明
- 用户风险披露

Q333：是否允许平台提供 API 交易？

允许，但需：

- API 安全
- 用户风险揭示
- 交易监控

Q334：是否可以运营 NFT 交易市场？

可以。MiCA 对 **非金融型 NFT** 管辖较宽松。
但必须：

- AML
- 风险披露
- 消费者保护

Q335：NFT 是否属于 MiCA 管辖？

单一 NFT → 不属于
可分割/批量发行 NFT → 可能属于 MiCA

Q336：是否允许运营 GameFi 平台？

可以，但需提交：

- 游戏内资产定义
- Token 分类
- 经济模型风险
- AML 风险

Q337：是否允许运营 RWA（实物资产代币化）平台？

允许，但取决于：

- RWA 是否等同于证券
- 是否构成 ART 或 EMT
- 是否涉及托管

Q338：是否允许代币化证券服务?

不允许使用 CASP 牌照。
必须申请 **MIFID II 投资公司牌照**。

Q339：是否可以将托管部分外包?

允许，但核心责任仍在 CASP 本身。
必须提供：

- 托管协议
- 资产分层说明
- 外包风险评估

Q340：平台类业务是否必须提供"退出计划（Exit Plan）"?

必须。
MiCA 要求所有高风险 CASP 提供：

- 退出流程
- 资产返还机制
- 客户通知机制
- 审计确认

第七章｜风险管理与 ICT 安全（Q341～Q380）

（适用于：交易平台、托管、经纪、咨询、撮合、订单执行、OTC 业务等全部 CASP 类别）

Q341｜芬兰 MiCA-CASP 风险管理框架必须包含哪些核心模块?

根据 FIN-FSA 与 MiCA 监管要求，风险管理体系需至少覆盖下列 10 个模块（必须文件化）：

1. **战略风险（Strategic Risk）**
2. **运营风险（Operational Risk）**
3. **市场风险（Market Risk）**
4. **流动性风险（Liquidity Risk）**
5. **信用风险（Counterparty Risk）**
6. **技术风险 / ICT 风险（ICT Risk / DORA）**
7. **网络攻击风险（Cybersecurity Risk）**
8. **钱包私钥管理风险（Private Key / MPC / HSM）**
9. **托管资产损失风险（Safeguarding Risk）**
10. **合规风险（Compliance / AML）**

FIN-FSA 特别强调：
风险管理负责人必须具备经验，不可仅由外包机构承担，外包仅可辅助但不可替代。

Q342｜芬兰监管是否要求 CASP 建立 "三道防线（Three Lines of Defense）"?

✓ 是，强制性（尤其是提供托管或交易平台的 CASP）
三道防线要求：

1. **第一道防线：业务部门（运营 + 技术）**
   - 实施风险控制
   - 执行交易监控 / 钱包权限

2. **第二道防线：独立合规团队（Compliance Officer / MLRO）**
    - 制定政策
    - 监管监控
    - AML/KYC 管理
    - STR 报告
3. **第三道防线：内部审计（Internal Audit）**
    - 必须独立
    - 可外包，但要满足 MiCA 独立性规定
    - 至少每年审计一次

FIN-FSA 会在面谈中确认：
是否为每条防线建立清晰的 SOP、汇报线、权限制度。

Q343｜芬兰 CASP 是否需要符合欧盟 DORA（数字运营韧性法案）？

✓ 是。DORA 将自 2025 年强制适用，MiCA CASP 属于受监管金融实体。
必须具备：

- ICT 风险管理策略
- 业务连续性计划（BCP）
- 灾难恢复（DRP）
- 渗透测试计划
- 网络攻击事件报告机制（重大事件需 24 小时内通知 FIN-FSA）

Q344｜托管类 CASP 在芬兰必须采用 MPC / HSM 吗?

MiCA 并未强制“必须 MPC 或 HSM”，但 **FIN-FSA 监管偏好如下：**

- ❗ **绝对不接受纯软件钱包单点密钥（Single Private Key）**
- ✓ **强烈偏好 MPC（多方安全计算）**
- ✓ **同级推荐 HSM（硬件安全模块）**
- ✓ “MPC + 冷备份 HSM” 为监管最佳实践

FIN-FSA 面谈必问：
“Describe your private key generation, storage, rotation, and access control.”

Q345｜芬兰监管是否接受第三方托管（Custody Outsourcing）？

可以，但必须满足：

- 外包不影响最终责任（CASP 仍负最终责任）
- 外包方必须符合等同资质
- 需签署 Outsourcing Agreement（含 SLA、审计权）
- 关键功能外包必须提前向 FIN-FSA 报告
- 客户资产风险不得因外包而增加

典型结构：
CASP 自有 MPC 钱包 + 第三方保险 + 独立监控节点

Q346｜芬兰 CASP 是否强制购买托管保险（Custody Insurance）？

不是强制，但 **FIN-FSA 非常鼓励购买**，尤其是托管服务和交易平台。
常见保险：

- Crime Insurance
- Cyber Insurance

- Digital Asset Custody Insurance
- Technology E&O

不购买保险 → 需提交更严格的风险缓解文件。

Q347｜Finn-FSA 对"资产隔离（Safeguarding of Assets）"的硬性要求有哪些?

必须做到：

1. **客户资产与公司资产分离**
2. **每日对账（Daily Reconciliation）**
3. **独立账户（Omnibus / Segregated）**
4. **明确的资金流规则与审批流程**
5. **客户提款需多重审批 + 多签（如 M-of-N）**
6. **对异常交易必须自动冻结、人工复核**

注意：
若 CASP 是纯经纪，不持有客户资产 → 可豁免部分托管要求。

Q348｜芬兰监管对"流动性风险管理"有哪些额外要求?

FIN-FSA 要求：

- CASP 必须证明可覆盖运营成本（至少 6 个月）
- 对自营风险进行限制（交易平台尤其重要）
- 建立 "Stress Test" 压力测试
- 资金储备需在 EEA 银行账户持有

如涉及 Order Execution / OTC，需提交：

- Counterparty Risk Matrix
- Settlement Risk Control（结算风险控制）
- Market Volatility Scenario（价格剧烈波动应对方案）

Q349｜ICT 关键系统必须部署在芬兰本地吗?

非强制，但需满足：

- 数据必须存储在 **EEA 区内**
- 若使用非 EEA 云服务商 → 必须提供充分的法律依据（GDPR + 附加控制措施）

FIN-FSA 常见通过方案：

- AWS / Google Cloud / Azure（欧盟地区节点）
- 本地混合部署（Hybrid Cloud）
- 数据加密（At Rest & In Transit）
- 加密密钥在 EEA 的 HSM 内管理

Q350｜FIN-FSA 是否会审核源代码?

不审查全部源代码，但会要求：

- 系统架构图（Architecture Diagram）
- API 权限矩阵
- 日志系统说明（Logging & Monitoring）
- 钱包系统说明（MPC/HSM 白皮书）
- 上线前第三方审计报告（如审计公司/网络安全公司）

如提供交易撮合服务 → FIN-FSA 会要求撮合逻辑说明。

Q351｜如何证明算法撮合系统不存在"自我交易 / 市场操纵"?

需要提交:

1. **撮合引擎逻辑文档（Matching Engine Logic）**
2. **反市场操纵机制（Market Abuse Prevention）**
3. **Price Integrity Controls（价格监控）**
4. **日志（可追溯与不可篡改）**

FIN-FSA 会重点检查:

- 是否允许内部账户进行对敲
- 是否提供"影子价格 / 内部参考价"
- 是否与外部流动性提供者（LP）存在利益冲突

Q352｜芬兰 CASP 是否必须对所有员工进行安全培训?

✓ 必须，每年至少一次。
培训范围:

- 信息安全
- AML/KYC
- 钱包安全
- 网络钓鱼防范
- 内部权限使用与违规报告
- 数据泄露预防

培训记录（Training Log）必须保存 **至少 5 年**。

Q353｜芬兰监管是否要求 CASP 启用"不可删除日志"（Immutable Logs）?

✓ 推荐，但未写死必须。
FIN-FSA 推荐:

- WORM（Write Once Read Many）日志
- 不可篡改的内部审计链
- 全量日志保存 5 年（至少）

如采用区块链方式存证 → 可加分。

Q354｜MPC 多方签名的"审批流程"是否需要提交?

✓ 必须，包括:

- 谁可以批准转账
- 几人签署（例如 2-of-3 / 3-of-5）
- 紧急权限（Emergency Access）
- 风险阈值（如≥10 BTC 需双方批准）
- 大额提款隔离（冷钱包流程）

FIN-FSA 最关注"滥用风险"和"单点失败风险"。

Q355｜DORA 是否要求芬兰 CASP 做 Red Team（红队）测试?

对于大型 CASP:

- **✓ 必须进行渗透测试**
- ✓ 可能被列入 Threat-Led Penetration Testing（TLPT）

对于中小型 CASP：

- ✓ 建议每年做一次渗透测试
- ✓ 提供网络安全评估报告即可

Q356｜芬兰 CASP 是否必须提交"业务连续性计划"（BCP）？

✓ 必须（MiCA + DORA 共同要求）
需包含：

- 灾难恢复点（RPO/RTO）
- 多地备份
- 核心员工应急名单
- 关键供应商替代方案
- "重大事件 4 小时内通知监管"机制

Q357｜如果 CASP 遭到黑客攻击，芬兰监管必须多久汇报？

根据 DORA：

- **重大 ICT 事件：24 小时内初步报告**
- **72 小时内详细报告**
- **1 周内提交最终事件根因报告**

Q358｜芬兰监管对"系统外包（ICT Outsourcing）"的要求？

必须提交：

- Outsourcing Registry
- SLA
- KPIs
- 数据备份与恢复方案
- 外包服务不可涉及关键权限
- 监管访问权必须包含（Regulator Access Clause）

Q359｜是否可将 KYC/AML 工具外包给第三方？

✓ 可以，但需满足：

- 审批前必须提交供应商尽职调查
- 外包不减轻 CASP 的最终责任
- CASP 必须有能力独立审核 KYC 结果
- 供应商必须符合 GDPR
- 需记录 Vendor Risk Assessment

常见外包工具：

- Sumsub
- Onfido
- Veriff（爱沙尼亚）
- Chainalysis / Elliptic（链上监控）

Q360｜FIN-FSA 是否允许 100% 自动化 KYC?

允许，但必须：

- 设置人工复核阈值
- 设置高风险国家自动升级流程
- 对制裁命中（Sanction Hits）必须人工决策
- 高价值交易需增强尽调（EDD）

Q361｜是否可以使用 Telegram / WhatsApp 作为客服渠道?

可用，但必须存档聊天记录并导入内部系统以满足 MiCA + GDPR 要求。
不能：

- 使用不可追踪的私聊
- 使用自动清除记录的消息（如自毁模式）

Q362｜芬兰监管是否允许算法自动冻结账户?

可以，但需遵守：

- 需明确风险阈值
- 冻结后需人工复核
- 不允许"无人工干预的永久限制"
- 必须在 Terms & Conditions 中写明

Q363｜是否需要提交内部权限体系（Access Control Matrix）?

✓ 必须。
包括：

- 钱包权限
- 后台操作权限
- 管理员权限
- 开发者权限
- 交易监控权限
- 数据访问权限
- 应急权限（必须隔离）

FIN-FSA 面谈会问：
"Who can change parameters of the matching engine?"

Q364｜FIN-FSA 是否要求 CASP 实施"职能分离（Segregation of Duties）"?

✓ 必须。
典型示例：

- 不能让同一个人：开发系统 + 审核交易 + 发起提款
- 钱包操作需多人审批
- 合规与业务需分开
- 风险管理不可兼任 CTO

Q365｜如何提交芬兰 CASP 风险登记册（Risk Register）?

需包含：

- 风险类别
- 风险评分（Likelihood × Impact）
- 风险负责人
- 风险缓解措施（Controls）
- 审核周期
- 监控日志
- 残余风险（Residual Risk）

仁港永胜可提供 **MiCA 官方可用 Risk Register（专业版）**。

Q366｜是否需要进行年度第三方安全审计？

✓ 强制性要求（MiCA Article 61）
审计内容：

- 网络安全
- 应用安全
- 钱包安全
- 交易系统
- 数据保护（GDPR）
- 运营流程

Q367｜芬兰监管对"链上监控（Blockchain Analytics）"的最低要求？

必须具备：

- 地址风险评分
- Mixer / Tornado Cash 检测
- Sanctioned Address 检测
- Darknet Market 检测
- Counterparty Identification（交易对手识别）
- Suspicious Address Alert（可疑地址报警）

须提供合规工具证据（Chainalysis/Elliptic/SCORECHAIN）。

Q368｜可否使用 DeFi 作为流动性来源？

高风险，FIN-FSA 基本不接受，除非：
✓ 仅作为"辅助流动性来源"
✓ 有风险限制（% 限额）
✓ 提供对手方评估与 KYC
✓ 智能合约需审计证明
✓ 不用于零售客户资产

Q369｜是否允许 CASP 进行自营交易（Proprietary Trading）？

MiCA 不鼓励，FIN-FSA 更保守。
允许但需：

- 不得损害客户利益
- 不得与平台撮合功能产生利益冲突
- 需对自营与客户交易完全隔离
- 需内部风控限制敞口

- 需向监管详细披露策略类型（不要求算法但需描述逻辑）

Q370｜托管与交易平台在芬兰是否允许同公司持有？

可以，但必须：

- 职能分离
- 权限分离
- 托管与撮合流程分开
- 不得影响订单公平性
- 提供独立风险控制体系

Q371｜是否必须有"客户赔付预案（Compensation Plan）"？

非强制，但 FIN-FSA 强烈建议：
内容包括：

- 托管损失赔付机制
- 技术故障赔付机制
- 交易回滚补偿机制
- 服务中断补偿机制

Q372｜是否必须进行反内部交易（Anti-Insider Trading）监控？

✓ 必须（MiCA Market Abuse 条款）
需提交：

- 内部观察名单
- "受限账户"机制
- 监控员工交易
- 员工申报制度

Q373｜市场操纵风险（Market Manipulation Risk）如何控制？

需提供：

- Wash trading 控制
- Spoofing 检测
- Pump-and-dump 监控
- Layering 检测
- Cross-exchange manipulation 检测
- 大额异常交易审查

Q374｜FIN-FSA 是否要求"安全事件演练"记录？

✓ 必须，包括：

- 演练计划
- 演练脚本
- 参与人员
- 演练报告
- 改进清单

Q375｜是否允许使用 AI 自动监控交易与风险?

允许，但必须：

- 提供可解释性（Explainability）
- 不可完全替代人工审批
- 设置人工复核机制
- 必须记录 AI 决策日志

Q376｜客户资产是否必须每日对账?

✓ 必须（Daily Reconciliation）
如提供托管 → 必须：

- 冷钱包
- 热钱包
- 冗余钱包
- 客户资产
- 自有资产

每日对账与记录。

Q377｜是否允许客户使用智能合约直接托管资产？（Self-Custody）

可以，但 CASP 不承担技术责任。
CASP 必须保证：

- 对智能合约风险有充分披露
- 不控制用户私钥
- 提供风险提示文档
- 不得误导客户"官方托管"

Q378｜是否必须记录所有钱包地址来源（Proof of Ownership）?

✓ 必须。
包括：

- 客户自有钱包
- 平台分配钱包
- 冗余钱包
- 热/冷钱包
- 交易对手钱包

需使用签名验证 + 区块链分析工具。

Q379｜FIN-FSA 是否允许使用多链钱包?

允许，但必须：

- 各链交易监控能力
- 各链风险评分系统
- 支持链上 AML 检测
- 对高风险链（如匿名链）需额外控制

Q380｜是否需要提交"年度安全路线图（Security Roadmap）"?

✓ 强烈建议（有助于加分）

包含：

- MPC 升级计划
- Tokenization 计划（如需）
- Cyber defense 战略
- 流量监控系统升级
- 风险模型优化

FIN-FSA 审查非常喜欢看到此文件。

第八章｜客户保护、运营规则与业务流程（Q381～Q430）

Q381｜芬兰 MiCA-CASP 对"客户保护（Investor & Consumer Protection）"的总体要求有哪些？

FIN-FSA 基于 MiCA Title V 要求 CASP 必须提供：

1. **透明披露机制（Disclosure obligations）**
2. **执行公平交易策略（Fair Treatment）**
3. **资产隔离（Safeguarding of Assets）**
4. **风险提示制度（Risk Disclosure）**
5. **订单最佳执行（Best Execution）**
6. **冲突管理机制（Conflict of Interest）**
7. **投诉处理机制（Complaints Handling）**
8. **合格投资者区分制度（Retail vs Professional）**

整体要求与传统金融机构非常类似，并更强调"损失提醒、风险提示和客户知情权"。

Q382｜FIN-FSA 要求 CASP 必须向客户披露哪些关键风险？

至少包括：

- 波动风险（Volatility Risk）
- 流动性风险（Liquidity Risk）
- 技术风险（Technical / Blockchain Risk）
- 托管风险（Custody & Private Key Risk）
- 市场操纵风险（Market Abuse Risk）
- 监管政策变化风险（Regulatory Risk）
- 稳定币风险（若涉及 EMT/ART）
- 智能合约风险（Smart Contract Risk）
- 加密货币可能归零风险

披露必须：

✓ 清晰

✓ 用普通消费者能理解的语言

✓ 不得隐藏在 Terms & Conditions 内

FIN-FSA 会审查是否存在误导性营销。

Q383｜客户资金进入与提款流程是否必须文件化？

✓ 必须。

文件至少包含：

1. 客户充值流程
2. AML/KYC 验证点
3. 链上地址验证逻辑
4. 提现审批机制
5. 多签或 MPC 权限流程
6. 异常提款冻结机制
7. 手续费与处理时间披露
8. 每日对账制度
9. 风险监控与自动报警

FIN-FSA 面谈必问：
"Please describe your end-to-end customer fund flow."

Q384｜客户资产可否与公司的自有资产混合存储?

❌ 不可以，MiCA 明令禁止。
必须做到：

- 客户资产独立钱包
- 公司资金独立钱包
- 明确区分热钱包与冷钱包
- 每日对账
- 记录所有内部划转流程

FIN-FSA 会抽查多签日志与操作记录。

Q385｜芬兰 CASP 对客户资产是否必须提供"清算优先权"?

✓ 必须遵守 MiCA 的"客户利益优先原则"。
若破产 → 客户资产不进入破产财产，CASP 需：

- 明确资产归属
- 提前准备破产隔离文件（Resolution Plan）
- 在合同中明确不会参与公司债务清算

Q386｜是否必须向客户提供"适当性测试"(Suitability Test）?

取决于业务类型：

业务类型	是否需要?
投资建议 Advice	✓ 必须
投资组合管理 Portfolio Mgmt	✓ 必须
交易平台运营	建议
经纪/订单执行	建议
OTC	强烈建议
托管	可选

FIN-FSA 会检查测试流程是否适用零售客户（Retail)。

Q387｜什么是"Best Execution"，芬兰 CASP 需如何满足?

指：**必须以客户最有利的条件执行订单**。
必须提供：

1. 最佳价格（Best Price）
2. 最佳成本（Best Cost）
3. 最佳速度（Best Speed）
4. 最佳执行地点（Best Venue）

5. 清晰披露执行策略（Execution Policy）
6. 订单优先队列规则（FIFO 或 Time Priority）

特别关键：
平台不可优先执行自营单。

Q388｜FIN-FSA 是否要求 CASP 定期公布"执行质量报告（Execution Quality Report）"?

✓ 类似 MiFID II RTS 27/28 要求，MiCA 也要求透明化。
必须至少年更：

- 订单执行地点
- 执行速度统计
- 订单成交率
- 价差情况
- 是否使用 LP（流动性提供者）
- 流动性分布

Q389｜能否在平台内设置"内部撮合（Internal Matching）"?

可以，但必须满足：

- 不得损害客户利益
- 不得隐藏撮合规则
- 不得优待特定账户
- 不得与自营交易混合
- 所有撮合规则需公开披露

FIN-FSA 重点检查是否存在 shadow dealing 或 wash trades。

Q390｜客户是否必须同意《风险披露声明》才能开户?

✓ 必须。
包括：

- 风险提示
- 资产损失可能性
- 市场操纵风险
- 技术风险
- 匿名交易风险
- 第三方协议风险（若使用外包）

须通过：

- 复选框确认
- 电子签署
- 审计可验证文件（存档）

Q391｜客户资产提款是否可加"冷却期（Cooling-off Period）"?

允许，但必须：

- 公告并同意
- 不能过长（一般 ≤24～48 小时）

- 不得阻止客户自由提款
- 仅用于风险控制或安全保护目的

FIN-FSA 审查重点：
"是否存在不合理提款限制？"

Q392｜平台是否可以提供"杠杆、保证金、期货、合约交易"？

是否允许＝取决于两条：

① 决定于 MiCA 牌照类型

MiCA CASP 不涵盖衍生品（Crypto Derivatives）。
若提供期货合约 → 可能需 MiFID 投资服务牌照。

② FIN-FSA 明确禁止面向零售客户的高风险杠杆

不允许：

- 永续合约（Perpetual Futures）
- 期权
- CFD

允许：

- **无杠杆现货交易（Spot）**

Q393｜是否可以给客户提供"收益计划 / Earn / Staking"产品？

FIN-FSA 极度严格，接近禁止：

- 大部分 Earn 等同"集体投资计划"或"存款替代物"
- 需符合 MiCA EMT/ART 稳定币发行要求
- 必须符合芬兰《投资基金法》
- 不得保证收益

如提供链上 staking → 需提供：

- 技术说明
- 风险披露
- 不承担链上损失

Q394｜客户是否可透过平台"自定义钱包地址"？

可以，但需：

- 地址验证（Proof of Address Ownership）
- 签名验证
- 风险评分（Chainalysis/Elliptic）
- 若属于高风险地址 → 冻结或要求说明

Q395｜平台是否需要限制高风险司法管辖区（FATF Blacklist）用户？

✓ 必须。
包括：

- 朝鲜
- 伊朗

- 缅甸（部分）
- 等 FATF 识别的国家

流程：

- 不允许开户
- 不允许存取款
- KYC 系统需自动拦截
- AML Officer 需记录决策

Q396｜FIN-FSA 是否允许"匿名交易"?

严格禁止。
要求：

- 完整 KYC（至少基本身份认证）
- 若交易量高 → 必须加强尽调（EDD）
- 若涉及匿名币（Monero 等）→ 足够风险控制或完全禁止

Q397｜客户投诉处理机制（Complaints Handling）必须包含哪些内容?

至少包括：

1. 投诉提交渠道（Email / Ticket）
2. 投诉记录（Logging）
3. 处理时间（一般 ≤15 天）
4. 投诉分类体系
5. 投诉升级机制（Compliance → Management）
6. 处理结果回复
7. 存档 5 年

FIN-FSA 会审查：
"是否真正由合规团队处理，而非客服自行处理。"

Q398｜平台可否进行"自动化账户封禁"?

可以，但条件：

- 有明确算法阈值
- 封禁后必须人工复核
- 若误封禁需快速恢复
- 记录日志并可追溯

Q399｜是否可以对客户施加"交易限额（Trading Limits）"?

允许且鼓励：

- AML 限额
- 风险限额
- 不同客户级别有不同限额（Retail vs Professional）

需披露：

- 限额机制
- 审批流程
- 风险因子

Q400｜是否需要向客户提供"交易记录导出功能"?

✓ 必须。
包括:

- 全部订单
- 成交记录
- 钱包地址
- 手续费
- 入金/出金记录
- 税务用途的账单（建议）

文件格式：CSV、PDF 必须提供。

Q401｜平台是否可以设置"强制止损 / 系统止损"?

允许，但必须:

- 完全透明
- 不得优先保护平台利益
- 不得触发不合理滑点
- 必须可验证且可审计

FIN-FSA 对"黑箱止损"持否定态度。

Q402｜订单簿是否必须公开?

若运营交易平台:
✓ 必须公开:

- 买卖盘深度
- 最新交易
- 成交量
- 价格区间

若 OTC → 订单簿可不公开，但需证明透明定价。

Q403｜CASP 是否必须提供"客户风险评分模型"文件?

✓ 必须。
模型需包含:

- 交易量
- 国籍
- 司法管辖区
- 行为模式
- 地址风险
- 资产来源
- 设备指纹

FIN-FSA 审查是否为真正可执行，而非装饰性模型。

Q404｜是否允许客户通过 API 交易?

允许，但必须:

- 限制速率（Rate Limit）
- 禁止滥用 API 进行拉盘
- 提交 API Key 管理机制
- 可随时撤销 API Key
- API 日志必须不可篡改

Q405｜FIN-FSA 对"定价机制（Pricing Methodology）"有什么要求?

必须公开以下内容：

- 定价来源
- 数据供应商
- 平均价格算法（如 VWAP）
- 价格更新频率
- 价格异常处理机制
- 与主要交易所的价格偏差监控

Q406｜平台是否必须提供"滑点控制（Slippage Control）"?

建议但非强制。
对于有撮合引擎的平台 → 滑点控制是必须的风险管理机制。
FIN-FSA 要求记录：

- 最大滑点阈值
- 用户同意机制
- 极端行情处理

Q407｜客户是否可通过代理人完成开户?

可以，但条件：

- 提供委托协议
- 必须对代理人进行 KYC
- 高风险代理需进行增强尽调
- 系统必须记录代理与用户关系

Q408｜是否可以将客户支持（Customer Support）外包?

可以，但 CASP 需：

- 提供投诉日志存档
- 提供培训材料
- 提供 SLA
- 确保外包不访问敏感数据（除非必要）
- 完全保留监管访问权

Q409｜是否可以删除客户交易历史?

绝对不可以。
MiCA + AMLD5 + GDPR 要求：

- 交易记录保存 ≥5 年
- 监管可随时抽查

- 若客户要求删除 → 可限于个人信息，不可删除交易记录

Q410｜平台必须支持哪些"客户账户类型"?

通常至少：

1. Retail（零售）
2. Professional（专业）
3. Institutional（机构）
4. High-risk（高风险分类）

每种类型有不同：

- 限额
- 风险控制
- 监控方式
- 权限

Q411｜是否必须向客户提供"赔付政策（Compensation Policy）"?

非强制，但建议提供：

- 交易错误
- 技术中断
- 服务延迟
- 提款延误

FIN-FSA 喜欢看到"客户保护文化"。

Q412｜平台是否可以支持"代币上线（Token Listing）"?

可以，但必须：

- 提交 Token Risk Assessment（MiCA 结构）
- 提供 KYA（Know Your Asset）报告
- 审查团队背景
- 审查智能合约
- 判断是否落入 MiCA EMT/ART 分类
- 完整市场操纵风险检查

FIN-FSA 会重点抽查该流程。

Q413｜是否可以支持高风险代币（如 Meme Coin）上线?

允许但风险更高。
需：

- 严格风险评估
- 明确风险披露
- 清楚区分零售客户
- 禁止误导性营销
- 必须符合 MiCA 市场操纵条款

Q414｜代币方是否可以付费上市？（Listing Fee）

可以，但：

- 必须公开披露上市费用
- 不得影响风险评估
- 不得因费用而忽略风险
- 必须避免"利益冲突"

Q415｜平台必须多久更新一次上市代币的风险等级？

建议每 3～6 个月重新评估一次。
以下情况需立即更新：

- 代币团队被监管调查
- 智能合约漏洞
- 重大黑客事件
- 市值暴跌
- 取消交易所上市

Q416｜平台是否可以暂停某代币交易？

✓ 可以，但必须：

- 提供暂停理由
- 告知客户
- 有内部审批流程
- 记录日志
- 确保暂停不损害客户利益

FIN-FSA 要求"非歧视性暂停机制"。

Q417｜是否允许"稳定币交易"？

允许，但必须符合 MiCA 稳定币规定：

- EMT（电子货币代币）
- ART（资产参考代币）

需符合发行人责任：

- 储备金
- 审计
- 赎回机制
- 披露义务

平台必须审查稳定币发行人是否合规。

Q418｜平台是否可以为客户提供"税务报告导出"？

可以，属于加分项。
尤其是芬兰对 Crypto Taxation 定义清晰，该功能更受欢迎。

Q419｜平台是否可以向客户提供投资策略或模型？

若属于"投资建议（Investment Advice）" → 必须具备相应 CASP 牌照类别。
建议避免：

- 投资回报承诺
- 精准预测
- 市场操纵可能性
- 定向推荐高风险代币

Q420｜FIN-FSA 对"自动交易 / 机器人交易（Bot Trading）"的限制?

允许，但需：

- 设置速率限制
- 不得造成市场操纵
- 提供人工审查机制
- 提供 Bot 活动日志
- 不得用于零售客户投资建议

Q421｜平台是否需要禁止"前置交易（Front-running）"?

✓ 必须。
需提供：

- 内部监控系统
- 员工行为限制
- 监控大额订单
- 匿名化订单簿

FIN-FSA 会检查：
"Does any employee have early access to customer orders?"

Q422｜平台是否可以通过"做市商（Market Maker）"提供流动性?

可以，但必须：

- 签订透明协议
- 公布利益冲突
- 不得操纵价格
- 不得与投机策略绑定
- 提供 LP 风险管理文件

Q423｜平台是否需要进行"订单簿压力测试"（Orderbook Stress Test）?

✓ 强烈建议。
内容包括：

- 深度骤减模拟
- 大额砸盘模拟
- 极端波动模拟
- 网络中断模拟

Q424｜是否可以支持"商家支付（Merchant Payment）"?

可以，但需：

- 反洗钱控制
- 资金流透明

- 商家 KYC
- 监控大额支付

Q425｜平台是否可以通过"推荐/邀请计划（Referral Program）"吸引用户?

可以，但不得：

- 误导用户
- 承诺收益
- 鼓励高风险交易
- 用 KOL 散布不实信息

应符合 MiCA 营销要求。

Q426｜平台是否可以对客户进行"重新 KYC（Re-KYC）"?

✓ 必须按风险等级周期性更新。
一般：

- 高风险客户：12 个月
- 中风险客户：24 个月
- 低风险客户：36 个月

Q427｜平台是否必须通过 GDPR DPIA（数据保护影响评估）?

✓ 建议，特别是：

- 使用生物识别 KYC
- 使用外包供应商
- 处理大规模数据
- 存储链上历史记录

DPIA 是 GDPR 的核心要求，FIN-FSA 亦会参考。

Q428｜是否可以使用区块链作为"客户身份存储系统"?

可以，但需：

- 不违反 GDPR"可删除权"要求
- 仅存储哈希
- 不存储个人身份直接数据
- 提供链上隐私保护机制

Q429｜平台是否可以支持"自动化风险警告弹窗"?

可以且建议：

- 大额交易提示
- 高风险代币提示
- 非常规行为提醒
- 可疑登录（IP/设备）提醒

FIN-FSA 认为这是"积极的消费者保护行为"。

Q430｜平台必须多久进行一次运营审计（Operational Audit）?

建议每年一次（至少每 12 个月）。
内容包括：

- 订单执行
- 客户保护
- 服务质量
- 投诉处理
- 运营风险管理
- 反洗钱流程
- ICT 营运
- 钱包管理流程

FIN-FSA 可要求在许可证后第一年提供额外运营审计。

第九章｜数据保护、GDPR、跨境数据 & 隐私合规（Q431～Q470）

本文由 仁港永胜（香港）有限公司 拟定，并由 唐生 提供专业讲解。

Q431｜芬兰 CASP 一定要遵守 GDPR 吗？是否有豁免？

✓ 必须遵守。
只要：

- 有欧盟/EEA 客户；或
- 在芬兰/欧盟境内设立实体；

就 **自动适用 GDPR**，不存在 MiCA 牌照机构的豁免。
MiCA ≠ 替代 GDPR，而是 **两部法规叠加适用**：

- MiCA 管"金融 & 牌照 & 投资者保护"
- GDPR 管"个人数据 & 隐私保护"。

Q432｜申请芬兰 CASP 时，是否需要提交正式的 GDPR 政策？

✓ 一般需要提交或至少在 RFI 阶段补交，包含：

1. **Privacy Policy（隐私政策）**
2. **Data Protection Policy（数据保护政策）**
3. **Data Retention Policy（数据保存政策）**
4. **Data Breach Procedure（数据泄露应对）**
5. **Data Subject Rights Procedure（数据主体权利流程）**

FIN-FSA 不会逐条当"隐私监管机构"来审查，但会检查：

> "你是否有合格的数据保护架构，并且能保护客户资料。"

Q433｜是否必须任命数据保护官（DPO – Data Protection Officer）？

视情况而定：

- 若 **大规模处理个人数据**、
- 或进行 **系统性监控**（KYC、交易监控、行为分析）、
- 或属于其他 GDPR 指定场景，

就 **应任命 DPO**，可以是内部人员，也可以是外部顾问。
对于大多数合规运营的 CASP，**配置 DPO 是强烈建议方案**，会加分。

Q434｜KYC 身份证/护照影像是否属于敏感数据？保存多久合规？

KYC 文档包含：

- 身份证/护照影像
- 地址证明
- 人脸识别/视频
- 税号/身份证号

全部属于 **高度敏感的个人数据**，必须遵守：

- 加密存储
- 权限极度收紧（只限 AML/合规/必要 IT）
- 防止非授权访问
- 只在实现 AML/KYC 目的所需的期限内保存

一般监管期望：

> AML 档案保存 **5 年或以上**（依据欧盟反洗钱指令）。

Q435｜客户要求"删除账户"和"抹去个人数据"时，CASP 必须全部删除吗？

❗ 不能简单"全部删除"。
需区分：

1. **出于法律义务必须保存的记录**
   - 交易记录
   - KYC/AML 记录
   - STR 报告
     👉 必须按 AML & MiCA 要求保留 ≥5 年，客户无权要求删除。
2. **其他不再需要的数据**
   - 营销数据
   - 不必要的元数据
     👉 客户可以要求删除或匿名化。

所以正确做法是：

> 执行"功能性删除/冻结"，保留满足监管要求的最小数据集，并记录处理过程。

Q436｜平台是否可以将客户数据用于"精准广告 & 营销"？

可以但极度敏感，需：

- 事先取得客户 **明确同意（Opt-in）**
- 清晰说明用途
- 提供"随时撤回同意"的机制
- 避免使用交易记录、敏感行为作为广告投放依据（会触碰 GDPR 风险）

对于 MiCA-CASP，**建议非常克制使用个性化广告**，以免变成监管"负面信号"。

Q437｜是否允许将 KYC 资料存放在海外（如香港、新加坡）服务器？

可以，但前提：

1. **数据出口符合 GDPR 第 44～49 条**
2. 存在：
   - 充分性决定（Adequacy Decision）；或
   - 标准合同条款（SCC）；或
   - 其他合法转移机制；

3. 做好 **Transfer Impact Assessment（TIA）**
4. 确保海外服务商具备足够安全措施

实务建议：
KYC 数据最好 **优先存在 EEA 区内数据中心**，仅在有必要时使用跨境备份。

Q438｜是否必须与所有第三方服务商签署 DPA（Data Processing Agreement）？

✓ 必须。
凡是：

- 代表平台处理个人数据的供应商（KYC、云服务、邮件、客服系统等），

都必须有 DPA，至少包括：

- 处理目的（Purpose）
- 处理范围与类型
- 技术和组织安全措施（TOMs）
- 分处理者（Sub-processor）管理
- 数据泄露报告机制
- 终止时数据返还/删除机制

FIN-FSA 在审查外包框架时，通常会顺带关注 DPA 是否合规。

Q439｜视频 KYC（Video KYC/Live KYC）在 GDPR 下有哪些额外要求?

包括但不限于：

- 录音录像保存期限说明
- 告知客户用途与法律依据（通常为 AML 法规义务 + 合同履行）
- 加密传输和存储
- 必须控制访问权限（只限 AML/合规团队）
- 如使用 AI 人脸比对 → 需更高程度透明 & DPIA

Q440｜是否需要对所有 KYC/AML 流程做 DPIA（Data Protection Impact Assessment）？

强烈建议，很多情况下其实是"事实上的强制"：

- 涉及大规模与系统性监控；
- 涉及敏感数据处理（生物识别、身份证件、地理位置等）；

GDPR 要求做 DPIA，用来：

- 分析风险
- 评估现有控制措施
- 设定额外保护措施

提交 MiCA 申请时可不附 DPIA 全文，但 **FIN-FSA 在 RFI 或后续检查中可能要求提供摘要或证明已完成 DPIA**。

Q441｜客户是否可以要求导出自己的个人数据?（数据可携权 Right to Data Portability）

✓ 客户有权：

- 要求导出自己提供的个人资料（如基础资料、KYC 信息）；
- 要求以 **结构化、常用、机器可读格式** 提供（如 JSON、CSV、PDF）；

但不包括：

- 内部风控模型
- 评分算法
- 其他第三方的机密数据

Q442｜GDPR 是否限制平台记录 IP、设备指纹、登录时间等信息?

可以记录，但需：

- 用于 **合法目的**（安全、AML、风控）；
- 告知客户会收集这类数据；
- 不滥用，如不恰当用于广告追踪；
- 遵守最小化原则（Data Minimisation）。

此类数据多用于：

- 异常行为检测
- 防止欺诈
- 安全审计

在 MiCA + AML 框架下，有合理的合法基础（Legitimate Interest + Legal Obligation）。

Q443｜GDPR 下是否必须支持"撤回同意"（Withdraw Consent）?

✓ 只要数据处理基于"同意"（Consent）而不是"法律义务"，客户有权随时撤回。
典型需支持撤回的场景：

- 营销邮件/推送
- 非必需 Cookie
- 用户行为分析工具（GA、Mixpanel 等）

对 AML、STR、交易记录 → 基本都基于"法律义务"，客户不能撤销。

Q444｜Cookie Policy 是否也会被 FIN-FSA 审查?

FIN-FSA 不是信息委员，但在以下场景会顺带检查：

- 你的网站/平台是否有清晰的 Cookie Banner；
- 是否对跟踪 Cookie 进行明确说明和选择；
- 是否存在"强制同意才能使用网站"的情况（Dark Pattern）；

虽然主要属于 **隐私监管机构** 责任，但 MiCA 审查时若 Cookie 明显违法，也会影响"整体合规印象"。

Q445｜平台是否可以把 KYC 视频交给第三方供应商长期保存?

可以，但必须：

1. 与供应商签署 DPA；
2. 确保数据存储地点与时间满足 GDPR & AML 要求；
3. CASP 仍需能控制数据（可导出、可删除非必要部分）；
4. 不允许供应商将 KYC 视频用于自有机器学习训练，除非客户明确同意；

建议： 关键 KYC 数据的"主控权"要在 CASP 手里。

Q446｜GDPR 允许将客户数据用于内部风控建模和风控算法优化吗?

可以，但需满足：

- 目的变更符合"兼容性"（Compatibility）原则；

- 尽可能使用去标识化/匿名化数据；
- 不用于歧视性决策（如针对国籍、种族的差别待遇）；
- 不通过单纯算法做具重大影响的自动决策（如永久封号、拒绝服务）——若有，需支持人工复核。

Q447｜GDPR 对"自动化决策（Automated Decision-Making）"有何限制？CASP 会踩雷吗？

GDPR 第 22 条限制"完全基于自动处理而对个人产生重大影响"的决策。
在 CASP 里可能踩雷的行为包括：

- 完全自动封号 & 永久禁止服务；
- 完全自动拒绝开户；
- 完全自动冻结资金且拒绝人工申诉；

合规做法：

- 自动决策 + 人工复核机制；
- 客户可要求人工审查其个案；
- 在隐私政策中明确告知。

Q448｜平台发生数据泄露（Data Breach）时，多久内必须向监管通报？

GDPR 一般要求：

- **72 小时内** 通知主管隐私监管机构（例如芬兰数据保护监察机构）；
- 若泄露对用户权利有高风险 → 需直接通知客户本人；

DORA & MiCA 叠加后：
严重 ICT 安全事件还必须向 FIN-FSA 通报。
仁港永胜通常会为客户统一设计：

> 一个"重大事件报告 Playbook"，同时满足 GDPR + DORA + MiCA 要求。

Q449｜平台是否可以与合作伙伴共享客户个人数据？（例如推荐计划、第三方钱包合作）

可以但受严格限制：

- 必须有法律依据（合同、合法利益、法律义务或同意）；
- 应与合作方签署 DPA 或数据共享协议（Data Sharing Agreement）；
- 告知客户会与哪些合作方共享；
- 不可用作对客户不利的商业推销或牟利行为；

特别提醒：
切忌"把用户数据当产品卖"。在欧盟，这是高风险违法行为。

Q450｜GDPR 对"数据保存期限（Retention Period）"有明确规定吗？

GDPR 的原则是：

> "只在达成目的所需的时间内保存。"

但 MiCA & AML 同时要求：

- 交易与 KYC 记录通常 **≥5 年**；
- 监管若有特别要求，甚至可以延长；

所以 CASP 应在政策中说明：

- 为满足 AML 与 MiCA 要求，某些数据将保存至少 5 年，且无法提前删除；
- 其他不必要的数据将定期清理或匿名化。

Q451｜是否要为 GDPR 设计独立的 Data Retention Schedule?

✓ 非常建议。
应列出：

- 各类数据（KYC、交易、客服记录、设备信息等）；
- 法律依据（MiCA/AML/GDPR）；
- 保存时长；
- 到期后如何处理（删除/匿名化）；

这份计划既是 GDPR 合规文件，也是 MiCA 审查时的"加分项"。

Q452｜GDPR 是否禁止使用区块链存储个人数据?

不禁止区块链，但需注意：

- 区块链"不可篡改"与 GDPR"可删除权"存在冲突；
- 不要在链上存储可识别个人的明文信息；
- 可以存储哈希（不可逆）、引用 ID、脱敏后的数据；

若项目涉及 **链上身份/SSI**，必须格外小心设计。

Q453｜客户通过 App 登录时，平台是否可以收集定位数据（GPS）？

可以，但需：

- 明确说明用途（例如风控、防欺诈）；
- 获得明确授权，特别是精确定位；
- 避免用于不恰当行为（如按地区差别定价）；

通常，IP + 设备指纹已足够风控，不强烈建议抓精确地理位置，除非确有必要。

Q454｜是否必须给客户一个 "隐私中心/Privacy Center" 来管理隐私选项?

不是硬性规定，但属于"良好实践"，包括：

- 下载数据
- 管理同意状态（对广告/分析工具）
- 管理邮件订阅
- 提交 GDPR 请求（访问/更正/删除）

对中大型 CASP，FIN-FSA 会更倾向看见成熟的隐私管理工具。

Q455｜GDPR 是否允许对不同国家客户进行"差异化合规"?

可以，但前提：

- 不得违反平等原则（如种族/宗教/性别歧视）
- 合规差异必须基于法律（例如有制裁或反洗钱要求）
- 对高风险国家客户实施更严格的 KYC/EDD 是被允许的

Q456｜平台是否必须保存 GDPR 合规活动的"文档记录"（Accountability）？

✓ 必须，这是 GDPR 的核心原则：

- DPIA 报告
- DPO 任命文件
- DPA 合同
- 数据泄露日志
- GDPR 请求处理记录
- 政策修订记录

这些文件将构成：

> "证明你认真遵守 GDPR 的证据"。

Q457｜是否需要在芬兰或欧盟任命"数据保护代表"（EU Representative）？

若公司：

- 虽不在 EEA 注册，但
- 有 EEA 客户且处理规模较大，

则 GDPR 要求任命一个 **EU Data Protection Representative**。
但本地设立芬兰 OY 的 CASP，一般自带此角色。

Q458｜平台可以将客户聊天记录（客服互动）用于训练 AI 吗？

可以但要格外谨慎：

- 必须做匿名化或去标识化处理；
- 不得保留能直接识别个人的信息（如姓名、身份证号等）；
- 最好在隐私政策中明确说明；
- 如果使用外部大模型供应商 → 需格外注意数据出境与机密性。

Q459｜平台是否必须支持用户查看自己的"风险评分/风险标签"？

法律不强制，但 GDPR 要求不允许完全黑箱化，尤其在风险评分影响服务提供时。
实务建议：

- 有一部分可解释信息（例如：交易模式、地理区域触发高风险）；
- 支持客户提出质疑并进行人工复核；

这也是 MiCA 所强调的"客户公平对待"一部分。

Q460｜GDPR 对"儿童/未成年客户"有什么要求？CASP 是否可以接纳未成年用户？

大多数 CASP 选择 **完全禁止未成年人开户**（通常要求 ≥18 岁）。
原因：

- KYC 难度高
- 适当性评估难以执行
- GDPR 对儿童数据保护更严（需父母同意等）

因此平台在 T&C 中通常写明仅接受成年自然人。

Q461｜平台是否要对"内部人员访问客户数据"进行审计和日志记录？

✓ 必须。
包括：

- 哪个员工访问了哪些客户数据

- 访问时间
- 访问理由
- 是否跨部门访问

这是 GDPR"最小授权 + 可审计性"原则的组成部分。

Q462｜能否使用美国大厂（如 Google Analytics）做流量分析?

可以，但风险略高：

- 自 Schrems II 判决后，欧美数据传输受限；
- 需配合 SCC、加密、IP 匿名化等控制措施；
- 欧盟已有对 GA 的监管案例；

更稳妥的是：

- 使用 **欧盟本地分析工具**；
- 或启用 GA 的增强隐私设置，并在 DPIA 中充分论证。

Q463｜平台是否需要对所有数据处理操作做"记录日志（Records of Processing Activities）"?

✓ GDPR 第 30 条要求必须维护 ROPA（个人数据处理活动记录），包括：

- 数据类别
- 处理目的
- 数据主体类别
- 接收方
- 安全措施

这是隐私监管抽查的重点文件之一。

Q464｜若平台计划未来上线新功能（例如 Web3 钱包、链上身份），是否需要重新评估 GDPR 风险?

✓ 必须进行"目的变更评估"：

- 是否新增了数据类别?
- 是否新增了处理目的?
- 是否需要新的法律依据?
- 是否要更新隐私政策 & DPIA?

这部分通常要形成一个"新功能合规评估表"。

Q465｜GDPR 是否会影响平台与执法机关、监管机构的数据共享?

不会阻止合法共享，但要求：

- 法律依据明确（如监管要求、法院命令、AML 报告义务）；
- 只共享必要数据（Data Minimisation）；
- 保留共享记录
- 通常无需提前征得用户同意（因为属于法律义务）。

Q466｜用户可以要求平台停止出于"合法利益（Legitimate Interest）"的数据处理吗?

用户有 **反对权（Right to Object）**，平台需：

- 评估自身合法利益是否高于用户权益；
- 若无法合理证明，需停止该类处理；

但 **针对 AML/MiCA 相关的处理**，通常以"法律义务"为基础，用户无权反对。

Q467｜平台是否需要进行定期 GDPR 内部审计？

强烈建议，每年一次：

- 检查所有流程是否符合政策；
- 检查外包是否合规；
- 检查数据泄露应对机制；
- 更新 DPIA & ROPA；

对于中大型 CASP，隐私监管可能会实地抽查，因此提前自查非常必要。

Q468｜GDPR 与 MiCA 之间是否存在冲突？如何处理？

通常不冲突，而是：

- MiCA 要求"必须收集 & 保存一定时长的数据"；
- GDPR 要求"尽量少收、少用、合理保存时间"；

处理办法：

- 以 MiCA & AML 要求建立数据的 **最低收集标准**；
- 在 GDPR 体系下说明"这是法律义务"；
- 同时不存在"超范围滥用"的行为。

如有争议，以"上位法与具体部门法"进行协调。

Q469｜能否将 GDPR/隐私工作完全外包给第三方法律事务所？

可以寻求外部顾问，但：

- **责任仍在 CASP 本身**；
- 内部必须有一个对 GDPR 有基本理解的负责人；
- 决策权不能完全交给外部；

MiCA + GDPR 的原则是：

> "你可以外包工作，但不能外包责任。"

Q470｜在芬兰申请 CASP 时，GDPR 合规部分是"必审项"还是"加分项"？

趋势上：已从"加分项"逐渐变为"隐性必审项"。

- 若隐私部分完全空白 → FIN-FSA 通常会发 RFI 提问；
- 若隐私架构成熟 → 监管会认为项目"整体治理成熟、风险意识到位"；

因此，**仁港永胜在设计芬兰 MiCA-CASP 申请方案时，都会把 GDPR/隐私块作为标准模块，而不是可选附件。**

第十章：监管互动、牌照维持、后续检查与 FIN-FSA 实务指南（Q471～Q520）
本章属于整个芬兰 MiCA-CASP FAQ 的 **收尾精华部分**，涵盖：

- FIN-FSA 补件方式（RFI）
- 面谈制度
- 牌照维持义务
- 年报/季报

- 主动披露机制
- 监管沟通技巧
- 牌照撤销风险点
- 仁港永胜（唐生）实务总结

本文由 仁港永胜（香港）有限公司 拟定，并由 唐生 提供专业讲解。

第十章｜监管沟通、牌照维持与监管实践（Q471～Q520）

Q471｜芬兰 FIN-FSA 审批 CASP 的典型 RFI（补件）节奏是什么？

一般约 2～3 轮：

第一轮 RFI：（通常 40～80 个问题）

- 资本 & 财务模型
- 业务流程图
- KYC/AML 流程
- 技术风险控制

第二轮 RFI：（通常 20～40 个问题）

- 客户保护
- 市场操纵防范
- ICT 风险细化（DORA）
- 钱包管理/SLA

第三轮 RFI（如有）：（10～20 个问题）

- 监管面谈后补充文件
- 决策确认
- 关键岗位人员背景核查

整体趋势比德国 BaFin 宽松，但比马耳他、爱沙尼亚严格。

Q472｜FIN-FSA 最常问的"6 类核心问题"是什么？

1. **业务模式是否会对零售客户产生过度风险？**
2. **平台是否"假去中心化，实中心化"？**
3. **KYC/AML 是否能抓住链上资金流？**
4. **市场操纵监控是否足够？**
5. **ICT（技术）风控是否符合 DORA？**
6. **关键人员（特别是 AML Officer 与 CTO）是否"可信赖 + 有能力"？**

Q473｜FIN-FSA 是否非常在意技术文件？（例如钱包架构、撮合引擎）

✓ 是。
尤其是技术风险（ICT Risks）、钱包安全、MPC/HSM，是芬兰重点关注点。
必须提交：

- System Architecture Diagram
- Wallet Key Management Diagram
- MPC/HSM 白皮书
- API 权限矩阵
- 日志保存策略
- 灾难恢复（DRP）计划

Q474｜FIN-FSA 在面谈（Interview）会问什么?

通常包括:

1. **业务理解**
2. **治理结构**
3. **AML 体系**
4. **ICT 与运营安全**
5. **客户保护 & 最佳执行**
6. **冲突管理（COI）**
7. **市场操纵控制**

最常见的问题示例:

- "Describe your end-to-end onboarding process."
- "Who approves withdrawals above 50,000 EUR?"
- "What if your CTO resigns suddenly?"
- "How do you detect wash-trading?"
- "How do you isolate client assets in a bankruptcy scenario?"

Q475｜关键人员面谈不过，会导致申请失败吗?

✓ 可能导致严重延迟甚至拒绝。
尤其关键角色:

- AML Officer（MLRO）
- Compliance Officer
- CTO（技术负责人）
- CEO（管理层）

FIN-FSA 会评估:

- 是否真正掌握流程
- 是否"表演式"回答
- 是否仅依赖顾问
- 是否有足够经验

仁港永胜会为客户提供 **模拟面谈训练（100+题库）**。

Q476｜芬兰 CASP 获牌后是否会有"事前通知义务"?（Ongoing Notification）

✓ 有。MiCA + FIN-FSA 双重要求。
必须在以下事项发生前/发生后 30 日内（视情况）通知监管:

- 董事/高层变更
- 持股结构变更
- 外包重大服务
- 系统升级
- 新增产品或新增代币
- 风险模型变更
- 信息安全事件（需更快）

Q477｜FIN-FSA 是否会对 CASP 进行"持续性检查"?

✓ 是。包括:

1. **现场检查（On-site Inspection）**
2. **书面检查（Off-site Review）**
3. **ICT 安全审计**
4. **AML 体系抽查**

频率通常为：

- 第一年度较密集
- 第二年起每年 1 次深度检查

Q478｜获牌后需要提交"年度报告 Annual Report"吗？

✓ 必须。
包括：

- 财务报表
- AML 年度评估
- ICT 年度评估
- 客户资产审计报告
- 内部审计报告
- 董事会年度声明（责任声明）

Q479｜是否要提交季度性监管报表（Regulatory Reports）？

视业务类型而定：

- 交易平台 → 通常需季度报表
- 托管服务 → 需月度/季度客户资金对账
- 投资建议/订单执行 → 按监管要求
- 所有 CASP → 每年至少一次 AML 报告

Q480｜FIN-FSA 会重点检查"客户投诉记录"吗？

✓ 是。
若投诉率高或投诉内容严重，会引发：

- 额外监管行动
- 现场检查
- 合规整改计划（Remediation Plan）

投诉流程必须：

- 可追踪
- 不可随意删除
- 定期报告

Q481｜"不活跃客户（Dormant Accounts）"是否需要单独管理？

✓ 需要。
必须建立：

- 识别规则
- 风险重评机制
- 冻结条件
- 资金返还机制（若长期不活跃）

FIN-FSA 会要求 CASP 明确 dormant 用户的风险控制方法。

Q482｜FIN-FSA 最关注的"市场操纵风险"有哪些?

重点五类:

1. **Wash Trading**（对敲）
2. **Spoofing & Layering**
3. **Pump & Dump**
4. **Cross-Exchange Manipulation**
5. **Insider Trading（内部交易）**

交易平台类 CASP 必须:

- 部署交易监控系统
- 留存日志
- 定期输出监控报告

Q483｜是否允许平台在获牌后"迅速扩展业务"?

可以，但:

- 所有新业务必须评估 MiCA 分类;
- 重大产品变更需提前通知 FIN-FSA;
- 不得绕过监管;

例如:

- 增加 OTC → 需更新风险评估
- 增加 staking → 若构成 EMT/ART 需新牌照
- 上线新代币 → 需做 KYA/KYT 报告

Q484｜平台若新增一个代币 Listing，是否必须通知监管?

不需要每一个代币都通知，但必须:

- 保留内部评估记录（KYA）
- 通过 Token Risk Assessment
- 分析是否落入 EMT/ART

若新增代币会改变整体风险结构 → 可能需要通知监管。

Q485｜FIN-FSA 会检查"钱包权限日志（Key Access Logs）"吗?

✓ 必检查。
特别是托管类 CASP。
包括:

- 谁访问了私钥/MPC 参数
- 访问时间
- 访问原因
- 是否超出权限
- 是否有双人审批记录

Q486｜若平台发生黑客事件，FIN-FSA 会采取什么行动?

可能措施:

1. 要求立即汇报（24 小时内）
2. 要求提交完整调查报告
3. 要求独立安全审计
4. 暂停业务
5. 限制提款
6. 要求补偿客户
7. 若管理严重不当 → 启动撤牌程序

Q487｜FIN-FSA 是否会检查"外包供应商"是否合规?

✓ 会。
FIN-FSA 要求 CASP：

- 对外包方进行尽职调查（Vendor Due Diligence）
- 保留合规记录
- 外包合同必须包含：监管访问权、数据保护条款、安全义务等
- 外包不可导致"失去对关键流程的控制权"

Q488｜平台若发生 CTO/MLRO 等关键人员变动，需要多久内报告?

通常：

- **事前通知**（重大角色必须先获监管批准）
- 若突发离职 → **立即报告**

FIN-FSA 非常重视关键岗位的连续性。

Q489｜CASP 是否可以临时使用外部服务商担任 MLRO?

不可以。
MiCA 要求 MLRO（反洗钱负责人）必须为：

- 实体内部员工（可不坐班，但需有实质职能）
- 熟悉芬兰 AML 法与 EU AMLD6 要求
- 有独立性，不受业务部门干预

Q490｜FIN-FSA 是否会检查"董事会会议记录"与"管理层会议记录"?

✓ 会。
监管重点：

- 会议是否定期举行
- 是否讨论关键风险事项
- 是否有 AML 报告汇报环节
- 是否对技术风险做决策
- 是否记录"客户保护"决策

这是判断治理水平的重要依据。

Q491｜若平台亏损，会影响 MiCA 牌照吗?

短期亏损不影响，只要：

- 有足够资本
- 业务可持续性分析充分

- 不影响客户保护
- 有财务恢复计划

但若：

- 长期亏损且无商业可行性
- 资金断裂导致无法运营

→ FIN-FSA 可能要求整改或限制业务。

Q492｜CASP 获牌后是否必须在芬兰本地雇员？

✓ 必须至少有：

- 1 位本地管理人员（高级管理）
- 1 位 AML Officer（可远程但需实质履职）
- 实际办公地址（可共享空间，但必须可现场检查）

Q493｜平台是否可以完全无实体办公室？（Fully Remote）

❌ 不可以。
MiCA 要求必须具备：

- 实际办公地点
- 可供现场检查的办公区
- 可访问的系统
- 合规文件存放地点

Q494｜监管是否允许 CASP 使用"虚拟办公室"或"只收信地址"？

❌ 不允许。
必须有 **真实可访问办公地址**。
虚拟办公会导致申请失败。

Q495｜FIN-FSA 会检查股东/UBO 吗？

✓ 会，尤其：

- 资金来源（Source of Funds）
- 资金合法性（Source of Wealth）
- 背景调查（PEP、制裁、犯罪记录）
- 避免不透明的离岸结构

不允许：

- 无法解释资金来源
- 高风险国家 UBO
- 多层匿名结构
- 名义股东/代持

Q496｜股东若为法人，需要提交哪些文件？

通常包括：

1. 注册证书
2. 董事/股东名单
3. 组织结构图

4. 资金来源证明
5. 财务报表
6. 董事与高层的 KYC 文件
7. 股东穿透文件（至自然人 UBO）

Q497｜哪些行为会导致 MiCA 牌照被暂停?

常见原因:

- 未按要求提交监管报告
- 风险管理严重缺失
- ICT 安全多次发生重大事故
- 洗钱报案义务未履行
- 未按要求通知监管关键变更
- 虚假陈述
- 误导消费者
- 资金混同

Q498｜哪些行为会导致 MiCA 牌照被撤销?

包括:

- 严重损害客户利益
- 重大洗钱事件
- 长时间无法经营
- 重大欺诈
- 关键人员缺失且无替代
- 故意对监管隐瞒风险
- 非法经营衍生品或高杠杆产品
- 大规模数据泄露但未报告

Q499｜平台是否必须设立"重大事件委员会（Incident Committee）"?

建议，但非强制。
包含:

- CEO
- CTO
- AML Officer
- Compliance Officer
- Security Lead

负责:

- 启动应急流程
- 报告监管
- 内部协调
- 客户沟通

Q500｜是否需要提交"年度 AML 报告（Annual MLRO Report）"?

✓ 必须，包括:

- STR 数量

- 客户风险等级变化
- 制裁名单监控情况
- 可疑地址识别情况
- 区块链监控报告
- 组织内部 AML 培训情况

FIN-FSA 此项非常严格。

Q501｜获牌后是否必须更新所有政策与流程？更新频率？

建议至少每年一次：

- AML/KYC
- 风险管理
- ICT 安全
- 市场操纵监控
- 客户保护政策
- 代币上架政策（若适用）

政策更新需要：

- 董事会批准
- 记录更新日志

Q502｜FIN-FSA 最喜欢什么风格的监管沟通？

三点：

1. **透明（Transparent）**
2. **主动（Proactive）**
3. **专业（Professional）**

他们不喜欢：

- 拖延
- 含糊
- 无证据支持的回答
- 敷衍一次性丢几十页文件

Q503｜是否要主动向监管汇报未来的产品路线图？

不是强制，但建议：

- 让监管知道你是"负责任、有治理能力的机构"
- 提前沟通能避免未来踩雷

例如：

- 上线新链
- 上线稳定币交易
- 新 KYC 工具

Q504｜FIN-FSA 是否允许"部分业务上线，逐步扩展"？

✓ 允许。
属于常见策略：

- 先获牌
- 再新增业务
- 再扩展功能
- 再上线更多代币

但每次变更都需更新风险评估。

Q505｜是否必须保存"董事会决策记录（Board Resolutions）"?

✓ 必须保存至少 5 年。
监管会重点检查：

- 董事会是否真正参与决策
- 是否理解风险
- 是否关注 AML

Q506｜FIN-FSA 是否会要求"独立内部审计（Internal Audit）"?

✓ 要求，但创始期可部分外包。

范围：

- AML
- ICT
- 内部控制
- 客户保护
- 市场操纵

Q507｜平台是否可以与监管保持电子邮件沟通?

可以，但：

- 必须使用公司邮箱
- 所有邮件必须存档（可审计）
- 若涉及重大事项建议正式信函

Q508｜申请失败后，还可以再次申请吗?

✓ 可以，但要谨慎。

- 第一次失败 = 风险标签
- 再申请需改进所有缺陷
- 最好由专业机构（如仁港永胜）重新规划

Q509｜若公司计划迁册至其他欧盟国家，是否需要重新申请 CASP?

视情况：

- 若仍在欧盟运营可保持 MiCA 护照
- 但监管主体可能需要变更
- FIN-FSA 会检查迁册理由与风险

Q510｜如何证明公司的"实际经营地（Mind & Management）"在芬兰?

必须有：

- 常驻管理层
- 董事会会议在芬兰举行
- 决策在芬兰做出
- 本地运营人员
- 实体办公室

虚拟"挂牌"不可行。

Q511｜是否可以由非欧盟人士担任 CEO/CTO/Compliance?

可以，但必须：

- 满足 Fit & Proper（适当人选）
- 无制裁
- 无金融犯罪
- 有相关经验
- 与公司有实质联系
- 能参加 FIN-FSA 面谈

Q512｜是否可以让集团公司提供"母公司担保"以满足资本要求?

不可直接替代"实缴资本"。
但可以：

- 作为补充财务稳定性证明
- 用于增强可持续运营能力

资本必须存于 EEA 银行。

Q513｜平台必须保存所有"系统日志"多久?

至少：

- 5 年（MiCA）
- 某些情况 ≥7 年（AML）

日志包括：

- 交易日志
- 钱包日志
- API 日志
- 访问控制日志

Q514｜平台是否可以暂时关闭业务（例如维护）？需要通知监管吗?

短期正常维护不需要汇报。
但需汇报：

- 若影响客户资产
- 若导致交易中断时间较长
- 若存在安全事件

Q515｜FIN-FSA 会重点检查哪些"客户保护文件"?

包含：

- 风险披露（Risk Disclosure）
- 执行政策（Execution Policy）
- 投诉管理程序
- 客户分类（Client Categorisation）
- 重大冲突管理政策
- 代币上架政策
- 资产隔离政策

Q516｜是否可以在社交媒体上进行"代币营销推广"?

可以，但必须：

- 不夸大收益
- 不作虚假陈述
- 明确风险
- 不误导零售用户
- 按 MiCA 营销规则披露必要信息

Q517｜监管最讨厌哪些"红牌行为"?

包括但不限于：

1. 杠杆交易、永续合约
2. 误导性广告
3. 使用假地址/虚拟办公室
4. 关键岗位"挂名"
5. 自营交易与客户冲突
6. 不披露代币风险
7. 未经过批准随意新增业务
8. 过度依赖外包而没有内部能力
9. 无法解释资金来源

Q518｜如何避免申请过程中"无限补件"?

关键方法：

- 提前准备完整申请包
- 由专业团队检查（仁港永胜）
- 模拟 FIN-FSA 审查过程
- 把所有文件整理成监管习惯的结构
- 不提交多余废话文件（监管讨厌冗长垃圾信息）

Q519｜平台如何在 FIN-FSA 眼中获得"高成熟度"评价?

表现为：

- 治理清晰
- 风险管理专业
- AML 独立与强势
- ICT 控制切实有效
- 钱包安全工业级（HSM/MPC）
- 清晰的客户保护文化

- 透明沟通
- 有持续合规投入

Q520｜仁港永胜（唐生）对申请芬兰 MiCA-CASP 的最终建议是什么？

（1）不要低估 FIN-FSA 的专业程度

他们非常懂区块链、懂风控、懂技术。

（2）不要假去中心化、实中心化

监管很容易识别。

（3）关键人员必须真实、强、有实质作用

不要出现"挂名式 MLRO/CTO/Compliance"。

（4）技术体系必须真实可落地，而不是 PPT

特别是钱包安全、日志、交易监控、数据保护。

（5）风险管理和市场操纵监控要提前设计完整结构

并非申请后才补。

（6）代币上架（Listing）要有专业的 KYA/KYT 模型

代币盲上线 = 风险。

（7）提前准备面谈，应对 70～100 道专业问题

仁港永胜提供完整模拟训练。

（8）申请文本必须是"欧盟监管语言"而非商业宣传语言

FIN-FSA 重视结构、准确性、逻辑性。

本文由 **仁港永胜（香港）有限公司** 拟定，并由 **唐生（Tang Shangyong）** 提供专业讲解。

关于仁港永胜 **– 您的 MiCA / CASP / EMI / VASP 全程合规伙伴**

About Rengangyongsheng – Your Global Regulatory Compliance Partner

---

一、公司简介｜Who We Are

仁港永胜（香港）有限公司
是一家专注于全球金融牌照与监管合规的专业顾问机构，在 **香港、内地及多个海外司法辖区** 拥有长期合作的律师事务所、会计师事务所、合规顾问及技术服务团队，为客户提供一站式的：

- 金融牌照申请与重组（MiCA CASP、EMI/PI、VASP、MSO、SFC 牌照等）
- 监管合规体系搭建（AML/KYC、风险管理、ICT 安全、内部控制）
- 商业计划书与监管沟通（BP、RFI 回复、面谈辅导）
- 银行及支付账户对接、跨境架构设计（Holding + SPV + 牌照实体）

我们更关注的是：

> **"项目能不能真正获批并长期活下去，而不是只拿一张纸。"**

二、核心优势｜Why Rengangyongsheng

1. 专注于金融与加密双领域交叉地带
我们长期深耕：

- 欧盟 MiCA CASP / EMT / ART
- EMI / PI（电子货币机构/支付机构）
- 虚拟资产服务提供商（VASP）
- 交易平台、钱包、托管、OTC、RWA、稳定币项目

2. 监管视角下重构商业模式
协助项目从监管视角重新设计：

- 业务边界（哪部分归 MiCA，哪部分归 MiFID、PSD2、EMD2、AML 等）
- 收费模式、产品设计、风险提示
- 客户分层（Retail / Professional / Institutional）

3. 从"拿牌"到"持续合规"的全生命周期服务

- 牌照可行性评估 & 司法管辖区对比
- 申请阶段：材料准备 + 线上提交 + RFI 补件 + 面谈演练
- 下牌后：年度合规、报告、内部审计、监管现场检查应对
- 架构调整：股权变更、业务迁移、集团重组

4. 文档体系与模板资源完备
围绕 MiCA / CASP / EMI / VASP 已沉淀大量可复用框架，包括但不限于：

- 《商业计划书（Business Plan）监管版》
- 《风险登记册（Risk Register）》
- 《AML/CTF 手册 + KYC 操作指引》
- 《ICT & 钱包安全政策（含 MPC/HSM 架构说明）》
- 《Token Listing 政策 & KYA/KYT 模板》
- 《监管问答包（Q&A Pack / RFI Pack）》
- 《董事会/治理架构文件套件》

这些模板会根据 **具体国家（如芬兰 FIN-FSA）、业务类型、公司规模** 进行定制化调整，而不是简单的"复制粘贴"。有需要客户可联系仁港永胜唐生定制服务。

三、针对芬兰 MiCA-CASP 的专项服务｜What We Do for Finland MiCA-CASP

围绕 **芬兰（MiCA）CASP 牌照**，仁港永胜可提供：

1. **项目前期评估与司法管辖区选择**
    - 对比芬兰、德国、马耳他、爱沙尼亚、奥地利、立陶宛等 MiCA 实施路径
    - 评估项目是适合申请"完整版 CASP"、还是"部分服务 + 护照扩展"
2. **申请材料总体打包设计**
    - 申请表 & 结构化附件
    - 股东/董事/核心人员 Fit & Proper 文件
    - 商业计划书（含 3～5 年财务预测）
    - 治理架构 + 三道防线（业务 / 风险&合规 / 内审）
3. **合规与风控体系搭建**
    - AML/KYC 政策与程序（结合链上监控工具，如 Chainalysis/Elliptic）
    - 风险管理框架（包括 Risk Appetite、Risk Register、控制矩阵）
    - 市场操纵防控机制（Wash Trading、Pump & Dump、Front-running 等）
    - 客户保护机制（Best Execution、适当性评估、投诉机制）
4. **ICT / 钱包 & DORA 合规设计**
    - 系统架构说明
    - 钱包托管架构（MPC/HSM、冷热钱包、权限矩阵、审计日志）
    - DORA 要求下的 ICT 风险管理、BCP/DRP、渗透测试规划

- 外包管理（云服务、KYC 服务商、技术供应商）

5. **监管沟通与面谈辅导**
   - 模拟 FIN-FSA 面谈问答（技术、合规、治理三条线）
   - 补件（RFI）策略设计：如何"答到点子上"又不过度暴露弱点
   - 监管提出整改要求时的"整改路线图"协助
6. **获牌后的持续服务**
   - 年度 AML 报告、年度合规报告、董事会材料
   - 内部审计、压力测试、政策年度回顾与更新
   - 协助应对现场检查、主题检查、数据与文档调阅

四、适合与我们合作的项目类型｜Who Should Talk to Us

- 计划以 **芬兰/欧盟为核心持牌中心** 的全球加密项目
- 有一定产品/技术基础，计划"从灰色走向完全合规"的 CEX / Wallet / OTC 平台
- 传统金融机构希望布局 **MiCA 合规数字资产业务**（证券行、券商、家族办公室、资产管理人等）
- 已持有其他国家 VASP/EMI/PI 牌照，希望 **增加一个欧盟 MiCA 合规支点** 的集团
- 有明确商业模式，却缺乏 **合规与监管沟通能力** 的 Web3 创始团队

如果你已经读完《芬兰（MiCA）CASP FAQ 大全》，
通常说明：你不是"随便试试"，而是真的在认真准备牌照与长期业务。

五、合作方式与下一步｜How We Work with You

1. **初步沟通（免费简报）**
   - 介绍项目结构、股东背景、拟开展业务
   - 初步判断是否适合走芬兰 MiCA-CASP 路线
   - 给出高层次方案与时间/预算区间
2. **方案设计与合规蓝图（付费顾问阶段）**
   - 输出《芬兰 MiCA-CASP 立项评估 & 路线图》
   - 明确：实体结构、资本安排、关键人员配置、时间表
3. **正式申请 & 监管互动阶段**
   - 全套文件制作与润色
   - RFI / 面谈 辅导
   - 直至牌照获批或监管有明确书面结论
4. **持续合规与升级阶段**
   - 年度/季度报送
   - 政策与业务迭代
   - 向其他欧盟成员国"护照通报"(Passporting)
   - 协助新增业务线（例如 RWA、支付、稳定币等）

六、联系方式｜Contact Rengangyongsheng

如需进一步了解 **芬兰 MiCA-CASP 牌照** 或其他国家/地区之
EMI / PI / CASP / VASP / BANK / MSO / SFC 等牌照方案，欢迎联络：

- **公司名称：** 仁港永胜（香港）有限公司
- **香港：** +852-9298 4213
- **深圳（微信同号）：** 159 2000 2080（唐生）
- **邮箱（Email）：** *tsy@cnjrp.com*
- **官网（Website）：** www.jrp-hk.com

注明：本文中的模板或电子档可以向仁港永胜唐生有偿索取。