

绿区专案 — 系统架构说明 (草案 v0.1)

ZD 数位转型委员会 · 编制日期: 2026-07-27

依据: 3 段语音描述 + PoC xlsx (4 模块 89 项) + 截图 (CSP 的 AI 方案 + 地端 LLM Gateway 16 项)

状态: 草案 / 待 TBD 项确认 · ZDT CONFIDENTIAL

一、文档说明

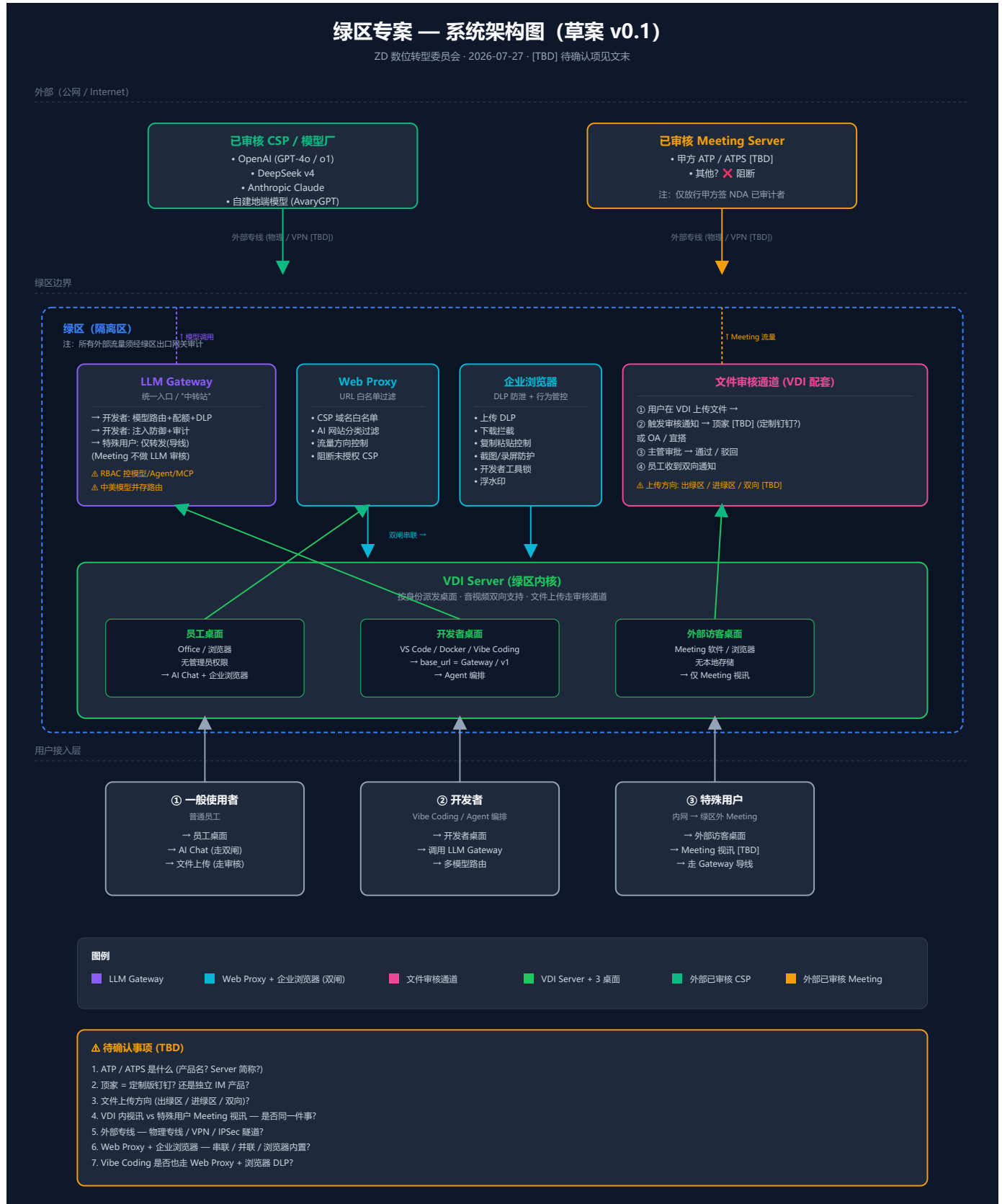
本文档是绿区专案**第一版架构说明**，由 3 个来源整合而成：

- 来源 A：甲方代表 3 段语音描述 (用户角色、绿区边界、LLM Gateway、文件审核)
- 来源 B：PoC测试项目清单.xlsx (5 sheet：封面、匿蹤、VDI、文件傳輸、企業瀏覽器；共 89 测试项)
- 来源 C：截图 "CSP 的 AI 方案 + 地端 LLM Gateway" (5 厂商对比表, 16 项测试)

△ 诚实交代：本草案中标注 [TBD] 的 7 处为语音中未听清 / 未明确的细节，已在文末 "TBD 清单" 列出。这些点必须在 v0.2 之前由甲方确认，否则会影响后续 RFP / PoC 实测。

二、整体架构图

下图整合 3 来源的视图 (外部 → 绿区边界 → VDI 内核 → 用户接入)



LLM Gateway

Web Proxy + 企业浏览器 (双端)

文件审核通道

VDI Server + 3 桌面

外部已审核 CSP

三、三层架构说明

3.1 外部层（公网）

类别	具体对象	状态
已审核 CSP / 模型厂	OpenAI · DeepSeek · Anthropic · 自建地端 AvaryGPT	✓ 放行
已审核 Meeting Server	甲方 ATP / ATPS Server	✓ 放行
其他 Meeting Server	Zoom / Teams 个人版等未审	✗ 阻断
其他 CSP / Model API	未签约的厂商	✗ 阻断

3.2 绿区边界层（4 大模块）

① LLM Gateway（统一入口 / "中转站"）

通道	走法	审核
开发者 → 模型调用	模型路由 + 配额 + DLP + 注入防御	完整 LLM 类审核
特殊用户 → Meeting	仅做转发（导线）	不做 LLM 类审核

② Web Proxy（URL 白名单）

- CSP 域名白名单
- AI 网站分类过滤
- 流量方向控制
- 阻断未授权 CSP

③ 企业浏览器（DLP 防泄）

- 上传 DLP + 下载拦截 + 复制粘贴控制 + 截图防护
- 开发者工具锁定 + 浮水印 + 扩展白名单
- 本机暂存关闭后清除

④ 文件审核通道（VDI 配套）

1. 用户在 VDI 上传文件
2. 触发审核通知 → 顶家 [TBD]（定制钉钉）或 OA / 宜搭
3. 主管审批 → 通过 / 驳回
4. 员工收到双向通知

3.3 用户接入层（3 类用户）

用户类型	桌面配置	主要场景	走网关
① 一般使用者	员工桌面	AI Chat · 文件上传	双闸（Web Proxy + 企业浏览器）
② 开发者	开发者桌面	Vibe Coding · Agent 编排	LLM Gateway（base_url）
③ 特殊用户	外部访客桌面	Meeting 视讯 [TBD]	LLM Gateway（仅转发）

四、6 模块 PoC 矩阵（厂商对比）

本节汇总 3 来源的测试项。来源 B 的 89 项 + 来源 C 的 16 项 = 共 **105 项**。下方按模块分组呈现， **是** 必要项， **视需求** /  **否** 表示该项是否关键。

4.1 匿蹤 (TrustOne) — 26 项 / 必要 22

类型	项目	必要	验证要点
功能	檔案/文字傳輸控制	是	受控管道、複製貼上、放行/阻擋、記錄
功能	檔案類型識別及控管	是	真實類型識別（不受副檔名影響）
功能	敏感訊息識別及控管	是	身分證字號/信用卡/自訂關鍵字
功能	圖像內容識別及控管	否	OCR 識別截圖/照片
功能	檔案靜態加密	是	端點/伺服器存放加密
功能	檔案傳輸加密	是	TLS 通道、封包側錄驗證
功能	上傳敏感內容識別及阻擋（DLP）	是	雲端服務上傳即時阻擋
功能	上傳檔案類型&大小限制	是	類型與大小上限
功能	惡意檔案/敏感文件下載攔截	是	EICAR + 敏感文件
功能	依風險評分及角色動態調整檔案權限	是	高風險裝置降級權限
功能	禁止使用個人帳號進行雲端服務	是	個人帳號阻擋/降為唯讀
管理	主管審核機制	是	外發申請核准/駁回 + 流程回查
管理	解密申請機制	是	申請+核准+記錄
管理	檔案浮水印	是	含使用者帳號/時間
管理	雙因子認證	是	登入/敏感操作第二因子
管理	統一身分平台串接	是	AD/統一帳號+群組權限
外發後控制	外發檔案有效期限控制	是	到期收件端無法開啟
外發後控制	開啟次數限制	否	超次拒絕開啟
外發後控制	外發後遠端撤回	是	已外發檔案立即失效
外發後控制	轉寄後持續受控	是	第三人開啟仍受控管+稽核
外發後控制	離線開啟行為控制	是	斷網時政策允/拒，連線補傳稽核
繞道測試	修改副檔名繞過測試	是	仍識別真實類型並控管
繞道測試	壓縮檔繞過測試	是	含加密壓縮仍識別
繞道測試	截圖防護	否	截圖/錄影阻擋或黑畫面
繞道測試	列印控制	是	阻擋或強制浮水印
審計	日誌審計	是	查詢/匯出/防竄改

4.2 VDI — 20 项 / 必要 14

类型	项目	必要	验证要点
功能	剪貼簿單向/雙向控制	是	本機→虛擬桌面允許，反向阻擋+記錄
功能	檔案傳輸（本機↔虛擬桌面）控制	是	依政策禁止下載/限制
功能	USB/周邊裝置重導向控制	是	USB 政策禁止/白名單
功能	列印控制	是	禁止或限定印表機+記錄
功能	螢幕浮水印	是	含使用者帳號/時間（防拍照外洩）
功能	截圖/螢幕錄製防護	否	本機端截圖/錄影驗證防護
功能	禁止使用個人帳號進行雲端服務	是	個人帳號阻擋
功能	多螢幕支援	否	雙螢幕延伸/解析度
功能	斷線重連與工作階段保持	是	網路中斷重連資料保留
功能	音訊傳輸（语音新增）	是	音訊雙向傳輸測試 [來源 A]
管理	依角色/部門指派桌面與應用	是	不同角色各自授權
管理	雙因子認證	是	登入 VDI 第二因子
管理	統一身平台串接	是	AD/統一帳號+群組
管理	使用者設定檔管理	否	不同次登入漫遊
效能與體驗	連線延遲與操作流暢度	是	文書/網頁/簡報延遲量測
效能與體驗	頻寬需求測試	是	平均+尖峰頻寬量測
效能與體驗	尖峰登入（boot storm）測試	是	大量同時登入穩定度
效能與體驗	同時在線數容量驗證	是	CPU/記憶體/儲存效能達標
效能與體驗	影像/3D 應用支援	否	影片+3D 流暢不破圖
審計	日誌審計	是	查詢+匯出
審計	工作階段錄影	否	高權限/敏感工作階段可錄影回放

4.3 文件傳輸 — 26 項 / 必要 24

类型	项目	必要	验证要点
功能	檔案/文字傳輸控制	是	受控管道、放行/阻擋、記錄
功能	檔案類型識別及控管	是	真實類型識別
功能	敏感訊息識別及控管	是	身分證/信用卡/關鍵字
功能	圖像內容識別及控管	否	OCR 識別
功能	檔案靜態加密	是	存放加密
功能	檔案傳輸加密	是	TLS 通道
功能	上傳敏感內容識別及阻擋（DLP）	是	雲端上傳即時阻擋
功能	上傳檔案類型&大小限制	是	類型與大小上限
功能	惡意檔案/敏感文件下載攔截	是	EICAR + 敏感文件

功能	依風險評分動態調整檔案權限	是	高風險裝置降級
功能	禁止使用個人帳號進行雲端服務	是	個人帳號阻擋/降唯讀
外發對象控制	外發對象身分驗證	是	信箱/簡訊/帳號驗證
外發對象控制	下載連結有效期與次數限制	是	連結效期+次數上限
外發對象控制	外發後撤回	是	已發送檔案/連結撤回
傳輸能力	大檔案傳輸效能與斷點續傳	是	10GB 中斷續傳達標
傳輸能力	傳輸完整性校驗	是	hash 對比一致
傳輸能力	與 OA/簽核流程串接	是	OA/宜搭核准自動放行
傳輸能力	跨網段/內外網檔案交換	視需求	單向/雙向政策+稽核
繞道測試	修改副檔名繞過測試	是	真實類型仍識別
繞道測試	壓縮檔繞過測試	是	加密壓縮仍識別
管理	主管審核機制	是	核准/駁回 + 回查
管理	解密申請機制	是	申請+核准+記錄
管理	檔案浮水印	是	含使用者帳號/時間
管理	雙因子認證	是	登入/敏感操作第二因子
管理	統一身平台串接	是	AD/統一帳號
審計	日誌審計	是	查詢/匯出/防竄改

4.4 企業瀏覽器 (PA / 亞信) — 17 項 / 必要 15

类型	項目	必要	验证要点
功能	上傳敏感內容識別及阻擋 (DLP)	是	瀏覽器內上傳雲端服務即時阻擋
功能	上傳檔案類型&大小限制	是	類型與大小上限
功能	惡意檔案/敏感文件下載攔截	是	EICAR + 敏感文件
功能	複製/貼上控制	是	受管網頁選取複製→本機應用阻擋
功能	截圖防護與螢幕浮水印	是	截圖阻擋+浮水印
功能	租戶限制 (禁止個人帳號)	是	個人帳號登入同服務阻擋
功能	開發者工具鎖定	是	F12 / 右鍵檢查停用
功能	擴充套件白名單管理	是	非白名單無法安裝/執行
功能	URL 過濾與分類控管	是	受限制類別網站阻擋+記錄
功能	本機暫存與關閉後清除	是	關閉後不殘留快取/暫存
管理	統一身平台串接	是	AD/統一帳號政策派送
管理	雙因子認證	否	登入/敏感系統第二因子
管理	集中政策管理與分群派送	是	依部門/角色派送, 即時生效
相容性與體驗	內部系統相容性 (OA/宜搭等)	是	核心系統登入+全流程正常

相容性與體驗	常用外部網站相容性	是	抽測版面/功能正常
相容性與體驗	效能測試	是	啟動/分頁/記憶體占用可接受
審計	日誌審計	是	查詢+匯出

4.5 LLM Gateway + CSP (Azure / 阿里 / Amazon+PA GW / 腾讯 / Google+PA GW) — 16 项

类型	项目	必要	验证要点
功能	支援雲/地模型算力整合及路由規則設定	是	雲端/地端模型算力整合、路由規則設定
功能	支援開發工具 API 的集成	是	Vibe Coding / Agent 等工具可整合
功能	多模型統一對接	是	單一入口調用多家模型
功能	能夠同時使用中美先進模型	是	中美模型並存路由（含合規）
管理	模型提供商調用失敗時切斷備用	—	主供商失敗時切換備援
管理	訪問速率限制（QPS）	—	按用戶/部門限制 QPS
管理	用戶配額限制	是	按用戶/部門設定調用上限
管理	依 RBAC 進行限制可以使用的模型/智能體/MCP	—	RBAC 控制模型/Agent/MCP 可用範圍
管理	熱更新不需要中斷服務	—	配置熱更新不中斷調用
管理	模型 API Key 管理並有加密機制	—	Key 集中管理+加密儲存
管理	與統一身份平台對接	—	AD/統一帳號認證
防護	Prompt 注入防護	是	越獄/Base64/多輪/間接注入
防護	敏感內容識別及阻擋（DLP）	是	PII/企業機密過濾
防護	敏感數據保留在本地	是	合規要求數據不出本地
防護	檢測大模型輸入/輸出的安全合規	是	輸入+輸出雙向合規檢測

来源 C 备注：本表 16 项来自截图 "CSP 的 AI 方案 + 地端 LLM Gateway"，与 PoC測試項目清單.xlsx 封面 R23 说明吻合 ("LLM Gateway 分頁依你的要求未包含在本檔")。本表 5 家厂商栏位为空，需 PoC 实测后填入支持情况。

五、模块与 3 源头对照表

模块	来源 A 语音	来源 B xlsx	来源 C 截图
匿蹤 (TrustOne)	—	26 项	—
VDI	音訊傳輸補充	20 项	—
文件傳輸 (TrustOne/飛馳雲聯/IPG)	—	26 项	—
企業瀏覽器 (PA/亞信)	—	17 项	—
LLM Gateway + CSP (5 厂商)	雙閘/中轉站/Meeting 導線	— (封面 R23 排除)	16 项
文件審核通道	頂家 [TBD] / OA 宜搭	—	—
外部 Meeting Server	ATP/ATPS [TBD]	—	—

六、待确认事项 (TBD)

1. **ATP / ATPS 是什么？** 是具体产品名？还是 Server 简称？需要产品资料确认。
2. **頂家** = 定制版钉钉二次开发？还是另一个独立 IM 产品？ZD 内部實際使用哪个？
3. **文件上传方向**：出绿区（员工→AI/外部） / 进绿区（外部下载到 VDI） / 双向？影响图上箭头方向。
4. **VDI 内視訊 vs 特殊用户 Meeting 視訊**：是同一件事（VDI 内开 Meeting）？还是两件事？架构图需明确。
5. **外部专线**：物理专线 / VPN / IPSec 隧道？影响架构图网络层画法。
6. **Web Proxy + 企业浏览器**：串联 / 并联 / 浏览器内置 Proxy？影响数据包流向箭头。
7. **Vibe Coding 是否走 Web Proxy + 浏览器**？还是只走 LLM Gateway？这关系到"雙閘"覆盖范围。

七、下一步建议

1. 甲方代表确认 TBD 7 项 → 出 v0.2 完整版架构
2. 根据 v0.2 架构，将昨日 RFP 与 PoC.xlsx 做 FR 矩阵对照 → 生成 RFP v1.1
3. 将本架构图嵌入 RFP 第 1 章"项目概述"，作为甲方对乙方的总体方案蓝本

文档结束 · 绿区专案架构说明草案 v0.1 · 2026-07-27 · ZDT CONFIDENTIAL

来源：语音描述 + PoC 測試項目清單.xlsx + CSP 的 AI 方案截图