

採購規範書(A522002113)

1. 品名：MCP 模型上下文協定場域規劃驗證委託案
2. 規格/功能需求及交付驗收項目：

項次	執行項目	執行說明	交付/驗收項目
1	MCP模型上下文協定場域規劃驗證委託案	一、MCP 場域環境與驗證情境規劃 依 AI+MCP 應用情境，規劃 MCP 場域驗證環境、MCP Server、MCP Tool 及驗證流程，並針對工具呼叫、節點協作、權限控管及異常行為等安全議題，規劃適用之驗證情境與測試方式。 二、研發技術場域介接與驗證規劃 配合工研院所研發之 MCP 攻防模擬測試技術、智慧決策模組技術及自動化安全驗證技術，規劃 3 項研發技術於 MCP 場域之介接方式、測試流程及驗證項目，並確認場域環境與介接需求，以支援後續場域整合驗證。 三、MCP 場域整合驗證 依規劃之 MCP 場域及驗證情境，介接工研院所研發之 3 項技術進行 Demo 整合測試，執行相關驗證情境並彙整測試結果，提出場域驗證結果及相關技術建議，以驗證 3 項研發技術於 MCP 應用場域之功能與可行性。	第一期：【MCP 場域驗證架構與情境規劃書】一式，內容至少涵蓋場域架構、MCP Server／MCP Tool 配置、驗證情境、3 項研發技術介接方式及測試流程。 第二期：【MCP 模型上下文協定場域規劃書及場域驗證技術報告】一式。
2	進度會議及維護	● 配合工研院需求進行進度會議及維護支援 ● 結案後持續保固至 116/4/30	

4. 交付驗收項目：

- 第一階段付款：廠商確認得標後，應於115/10/30前完成MCP場域驗證架構、驗證情境及測試流程規劃，並交付【MCP場域驗證架構與情境規劃書】一式。經工研院確認場域規劃內容符合本採購規範需求且驗收合格後，支付契約價金第一期款60%。
- 第二階段付款：廠商應於115/12/10前，完成與工研院所研發之MCP攻防模擬測試技術、智慧決策模組技術及自動化安全驗證技術等3項技術之Demo整合測試，並交付【MCP模型上下文協定場域規劃書及場域驗證技術報告】一式。經工研院確認場域整合驗證成果符合本採購規範需求且驗收合格後，支付契約價金第二期款40%。

5. 廠商配合項目：

- 得標廠商需提供顧問諮詢，若有未詳盡事宜得標廠商得全力配合委託方進行補充。
- 廠商須具備與工研院資安團隊合作之經驗。
- 廠商須配合工研院進行場域規劃、技術介接、整合驗證及相關技術討論與支援。
- 結案後，廠商應無償提供驗證場域相關技術支援至116/4/30。