

## 採購規範書(A522001220)

1. 品名：量子安全通訊與量子金鑰分配驗證方法研析委託案

2. 說明：

為了因應量子計算帶來的資安威脅，並解決傳統 QKD 網路架構中「可信節點 (Trusted Node) 容易成為駭客攻擊目標」的資安風險，擬委託協助設計具備「去信任化」特性之多路徑路由與秘密分享機制，研析量子模擬驗證，確保其設計的多路徑或秘密分享金鑰機制能夠於軟體定義 QKD 模擬平台上，作為後續技術研發之依據。

3. 功能/需求規格

序號	委託項目	項目說明	驗收標準
1	啟動會議及定期進度會議	於計畫決標後召開專案啟動會議，確認計畫執行目標、工作項目及時程規劃，並定期召開進度會議，追蹤執行成效並依會議決議辦理後續事項。 (得標後 10 個工作天內)	完成專案啟動會議並提供相關佐證
2	演算法與機制設計研析	研析多路徑金鑰傳輸與秘密分享機制，透過將量子密鑰拆分並經由不同節點路徑傳輸，確保即使部分中間節點遭攻陷，攻擊者亦無法還原完整密鑰。 (115/08/10 提交)	量子安全通訊報告 1 式
	技術與協定驗證研析	研析量子金鑰分配相關協定(QKD) 機制，建立驗證情境及評估，並進行量子通訊安全或多路徑機制之功能測試與專業技術驗證分析，分析 QKD 於不同通訊情境下之運作特性、安全需求及應用可行性，並提供驗證結果分析。 (115/12/10 前繳交)	QKD 模擬驗證分析報告 1 式

4. 驗收付款

- 第一階段付款：廠商確認得標後 **10 個工作天內**與工研院進行啟始會議，會議確認執行項目。提供會議召開佐證資訊後即完成驗收，合格後十個工作日內**支付總額 50%**。
  - 驗收請款：以完成啟始會議召開，並提交開會佐證資料作為本項驗收請款證明。
- 第二階段付款：**115/12/10 前**交付【量子安全通訊報告 1 式】及【QKD 模擬驗證分析報告 1 式】，經驗收合格後十個工作日內**支付尾款總額 50%**

5. 訓練：有 無

6. 保固：有 無

7. 服務：有 無

- 配合本計畫執行需求，為研析量子安全通訊相關技術及多路徑金鑰分享機制，需借重具量子通訊專業領域知識與研究經驗之專家學者提供技術研析與專業建議，作為後續技術研究、驗證分析及發展規劃之重要依據。
- 若有未詳盡事宜得標廠商得全力配合委託方進行補充。