TAICS

TAICS TS-0053 v1.0 : 2023

5G Open RAN資安測試規範

Cybersecurity test specification for 5G Open RAN

2023/07/20

社團法人台灣資通產業標準協會

Taiwan Association of Informationand Communication Standards

5G Open RAN 資安測試規範

Cybersecurity test specification for 5G Open RAN

出版日期: 2023/07/20

終審日期: 2023/06/20

誌謝

本規範由台灣資通產業標準協會－TC5 網路與資訊安全技術工作委員會所制定。

TC5 主席：神盾股份有限公司 張心玲 副總經理

TC5 副主席：財團法人工業技術研究院 黃維中 副所長

TC5 副主席：財團法人資訊工業策進會 蔡正煜 主任

TC5 副主席：財團法人電信技術中心 林炫佑 副執行長

TC5 行動通訊資安工作組組長：財團法人資訊工業策進會 柯盈圳 組長

技術編輯：財團法人資訊工業策進會 蔡宜學 技術經理

此規範制定之協會會員參與名單為(以中文名稱順序排列)：

中華電信股份有限公司、仁寶電腦工業股份有限公司、友達光電股份有限公司、台灣是德科技股份有限公司、正文科技股份有限公司、安立知股份有限公司、亞旭電腦股份有限公司、和碩聯合科技股份有限公司、英業達股份有限公司、香港商南德產品驗證顧問股份有限公司台灣分公司、神盾股份有限公司、財團法人工業技術研究院、財團法人資訊工業策進會、財團法人電信技術中心、啟碁科技股份有限公司、國立中正大學、國立陽明交通大學、國立臺北大學、智易科技股份有限公司、華電聯網股份有限公司、雲達科技股份有限公司、遠傳電信股份有限公司、德凱認證股份有限公司、緯穎科技服務股份有限公司、趨勢科技股份有限公司、耀登科技股份有限公司

本計畫專案參與廠商(法人)名單為(以中文名稱順序排列)：

宏達國際電子股份有限公司、緯創資通股份有限公司

本規範由數位發展部支持研究制定。

目錄

前言

本規範係依台灣資通產業標準協會(TAICS)之規定，經技術管理委員會審定，由協會公布之產業標準。

本規範並未建議所有安全事項，使用本規範前應適當建立相關維護安全與健康作業，並且遵守相關法規之規定。

本規範之部分內容，可能涉及專利權、商標權與著作權，協會不負責任何或所有此類專利權、商標權與著作權之鑑別。

引言

全球電信事業深刻感受到需要透過新的 Open RAN 的網路標準規範，達成更具競爭性與動態彈性的無線接取網路(Radio Access Network, RAN)供應鏈，積極推動 Open RAN 的網路架構以打破過去軟硬體高度整合的常態。Open RAN 的網路架構將整個硬體架構分成無線電單元(Radio Unit, RU)、分散單元(Distributed Unit, DU)、集中單元(Central Unit, CU)等，與不同層之間的傳輸介面與控制管理軟體。以 Open RAN 開放式的介面軟硬體架構，實現 5G 快速彈性化布署與客製化的服務，讓電信事業可以更快速的布署應用服務，並達成降低設備成本的目標。

在 Open RAN 標準化與開放過程中，需要透過眾多產業間的合作與溝通，以便在全球推動無線開放網路、軟體和虛擬化的目標。過去所有技術與介面大多由電信設備大廠統籌負責，一旦發生問題，負責之對象明確。Open RAN 改變傳統電信基地臺由國際大型電信設備商壟斷的狀況，但也隨著開放式架構的網通設備「白牌化」後，硬體軟體整合會有軟體相容性問題。市場也擔心開放架構會不會讓資安漏洞更多，且一旦出現資安疑慮，更會無從查起，這也讓資安問題更加複雜化。

為了解決 5G 開放式架構的資安議題，開放式無線接取網路聯盟(O-RAN Alliance)於 2021 年成立安全焦點小組(Security Focus Group, SFG)，並於 2022 年正式成為第十一工作小組(Working Group 11, WG11)之安全工作小組(Security Working Group, SWG)，專注於制定 Open RAN 網路產品的安全架構和安全保證規範，訂定開放式無線接取網路安全架構與框架，同時也致力於開放測試與整合中心(Open Testing and Integration Centre, OTIC)，推動產品資安保證評估驗證程序。

有鑑於 5G 多元應用型態於國內佈建獨立組網(Standalone, SA)系統架構時需要依賴 5G Open RAN 基地臺，在數位發展部數位產業署「5G 資安防護系統開發計畫」的支持下，資策會資安所團隊參考國際標準作法第三代合作夥伴計畫(The 3rd Generation Partnership Project , 3GPP)的安全性工作群組(SA3 Security)及無線接取網路聯盟(O-RAN Alliance)的安全工作小組(Security Working Group, SWG)訂定之 5G 系統通訊產品資安確保標準，制定相關的資安測試細節，並於台灣資通產業標準協會進行產業標準制定，以凝聚相關產、官、學、研各界共識。

「TAICS TS-0053 5G Open RAN 資安測試規範」(以下簡稱本測試規範)，參考 TAICS TR-0025 v1.0「5G Open RAN 資安研究報告」及 TAICS TS-0035 v2.0「5G 基地臺資安測試規範 v2」與無線接取網路聯盟(O-RAN Alliance)之標準規範，訂定 5G Open RAN 資安測試細節。本測試規範具體明列資安檢測之測試項目、測試條件、測試方法與檢測結果等事項，俾利基地臺製造商、系統整合商及 5G 資安檢測實驗室等作為相關產品檢測技術的測試要求。

1. 適用範圍

本測試規範訂定 5G 獨立組網 (Standalone, SA)之 Open RAN (Open Radio Access Network) 系統架構下包含 Non-RT RIC、Near-RT RIC、O-CU、O-DU 與 O-RU 網路元件之資安測試實施要求。5G 獨立組網(SA) 之 Open RAN 系統架構引用第三代合作夥伴計畫(3GPP)以及開放式無線接取網路聯盟(O-RAN Alliance)所定義之架構，即由用戶設備(UE)、Non-RT RIC、Near-RT RIC、O-CU、O-DU 與 O-RU 及 5GC 所組成，如下圖 1 所示。本測試規範之適用範圍包括圖 1 之紅框標註部分。

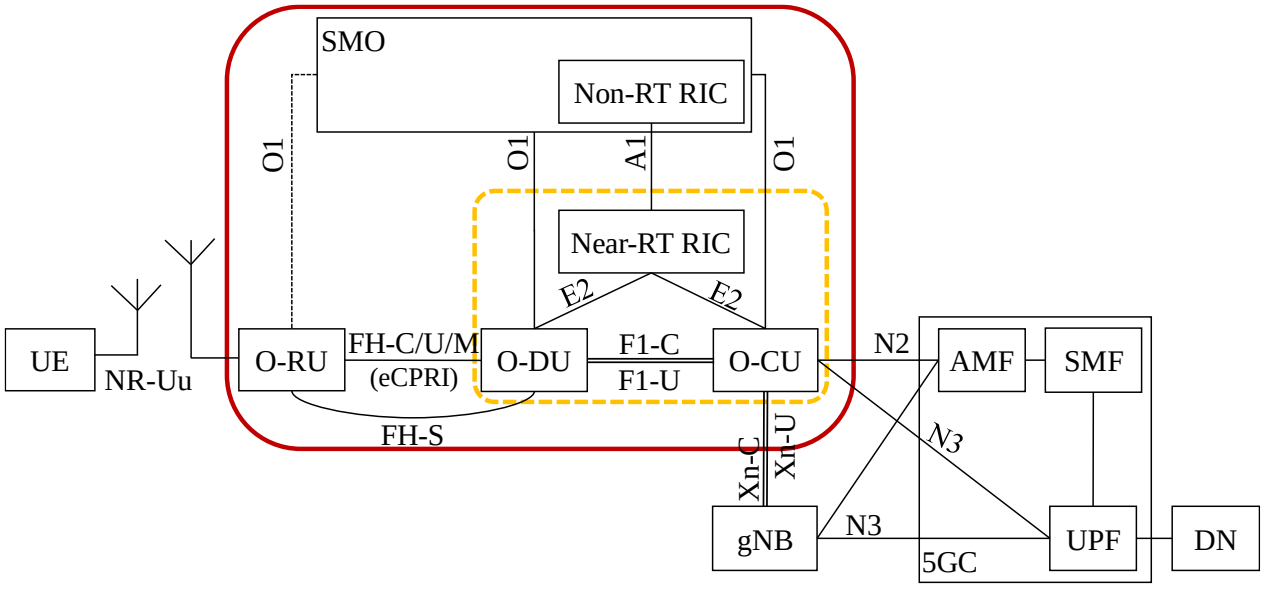


圖 1 Open RAN 系統架構

*註圖中之網路元件與介面用語定義於第 3 節

**可能無實體拆分的網路元件標註於橙色虛線框部分

2. 引用標準

下列標準因本規範所引用，成為本規範之一部分。有加註年份者，適用該年份之版次，不適用於其後之修訂版 包括補充增修 。無加註年份者，適用該最新版 包括補充增修。

[1] TAICS TR-0025 v1.0:2022, “5G Open RAN 資安研究報告”

[2] TAICS TS-0035 v2.0:2021, “5G 基地臺資安測試規範 v2”

[3] 3GPP TS 38.401-h40, “NG-RAN Architecture description”

[4] 3GPP TR 38.801-e00, “Study on new radio access technology: Radio access architecture and interfaces (Release 14)”

[5] 3GPP TR 38.806-f00, “Study of separation of NR Control Plane (CP)and User Plane (UP)for split option 2;(Release 15)”

[6] 3GPP TR 38.816-f00, “Study on Central Unit (CU)- Distributed Unit (DU) lower layer split for NR (Release 15)”

[7] 3GPP TR 33.818-h10, “Security Assurance Methodology (SECAM); and Security Assurance Specification (SCAS)for 3GPP virtualised network products (Release 17)”

[8] 3GPP TS 33.511-h31, “Security Assurance Specification (SCAS) for the next generation Node B(gNodeB)network product class (Release 17)”

[9] 3GPP TS 33.523-i00, “5G Security Assurance Specification (SCAS); Split gNB product classes (Release 18)”

[10] 3GPP TS 33.117-h20, “Catalogue of general security assurance requirements (Release 17)”

[11] 3GPP TS 33.501-h80, “Security architecture and procedures for 5G system (Release 16)”

[12] 3GPP TR 33.916-g00, “Security Assurance Methodology (SCAS) for 3GPP network products (Release 15)”

[13] 3GPP TR 33.926-h60, “Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes (Release 17)”

[14] 3GPP TS 33.210- h10, “3G security; Network Domain Security (NDS); IP network layer security (Release 17)

[15] O-RAN WG11, “O-RAN Security Test Specifications 3.0”

[16] O-RAN WG1, “O-RAN Architecture Description 8.0”

[17] O-RAN WG11, “O-RAN Security Threat Modeling and Remediation Analysis 5.0”

[18] O-RAN WG11, “O-RAN Security Requirements Specifications 5.0”

[19] O-RAN WG11, “O-RAN Security Protocol Specification 5.0”

[20] O-RAN TIFG, “O-RAN End-to-end Test Specification 4.0”

3. 用語及定義

下列用語與定義適用於本規範。

3.1 第三代合作夥伴計畫 (The 3rd Generation Partnership Project, 3GPP)

是一個成立於 1998 年 12 月的標準化機構，該機構設立的原初目的在推廣以全球行動通訊系統(Global System for Mobile communications, GSM)規格為基礎的國際行動通訊 2000(International Mobile Telecommunication-2000, IMT-2000)技術規範，提出一個能持續演進強化的國際通用技術標準規格，並於 2018 年 6 月與 2020 年 7 月正式完成 5G 獨立組網 (Standalone, SA) 第 15 版本 (Release 15) 以及第 16 版本 (Release 16) 的標準制定。目前其成員包括歐洲電信標準化協會(European Telecommunications Standards Institute, ETSI)、日本無線電產業與商務協會(Association of Radio Industries and Business, ARIB)、日本電信技術委員會(Telecommunication Technology Committee, TTC)、中國通訊標準化協會(China Communications Standards Association, CCSA)、北美通訊產業解決方案聯盟(Alliance for Telecommunications Industry Solutions, ATIS)、韓國電信技術協會(Telecommunication Technical Assembly, TTA)，以及印度電信標準發展協會(Telecommunications Standards Development Society, India, TSDSI)都簽署加入這個合作性協議中。

3.2 開放式無線接取網路聯盟 (Open Radio Access Network Alliance, O-RAN Alliance)

是一個成立於 2018 年 2 月的標準化機構，該機構由雲端無線接取網路聯盟(Cloud Radio Access Network Alliance, C-RAN Alliance)與 xRAN 論壇(xRAN Forum)兩個組織合併組成，以推動在全球無線網路方面的開放網路、軟體和虛擬化目標。在 Open RAN 標準化與開放過程中，需要透過眾多產業間的合作與溝通，以便在全球推動無線開放網路、軟體和虛擬化的目標。如透過開放性無線接取網路政策聯盟(Open RAN Policy Coalition)、開放測試與整合中心(Open Test and Integration Center, OTIC)、電信基礎架構專案(Telecom Infra Project, TIP)與開放網路基金會(Open Networking Foundation, ONF)和

Linux 基金會(Linux Foundation)以及全球行動通訊系統協會(Groupe Speciale Mobile Association, GSMA)等不同層面的單位各自投入發展開放式軟硬體的架構。

3.3 安全保證規範(Security Assurance Specification, SCAS)

涵蓋 O-CU、gNB 及 5GC 的七大資安威脅面向與相關資安測試案例，針對生產製造的行動通訊裝置進行合規檢測，並由資安實驗室針對設備的弱點進行規範檢測及防駭漏洞檢測等兩階段資安檢測。

3.4 網路設備安全保證方案 (Network Equipment Security Assurance Scheme, NESAS)

包含了設備供應製造商的開發與產品生命週期之認證、測試實驗室之認證、網路設備之安全性測試評估規範，針對支援第三代合作夥伴計畫(The 3rd Generation Partnership Project, 3GPP)定義功能網路產品的供應商構建安全認證框架，以提升行動產業的安全層級。並由全球行動通訊系統協會(Groupe Speciale Mobile Association, GSMA)負責管理、制定並定期修訂規範內容。

3.5 用戶設備 (User Equipment, UE)

由通用積體電路卡(Universal Integrated Circuit Card, UICC)和移動式設備(Mobile Equipment, ME)組成(1)，其中移動式設備可進一步由處理通訊功能的移動式終端(Mobile Termination, MT)和終端設備(Terminal Equipment, TE)組成。

3.6 gNB/gNodeB (Next Generation NodeB)

乃指 3GPP 5GNR 系統架構中，固定在一個地方的多通道雙向無線電傳送機，提供用戶設備(UE)雙向無線通訊，依據發射功率可以分為大型基地臺(Marco Cell)以及小型基地臺(Small Cell)。大型基地臺搭載巨量天線(Massive antennas)，主要布建位置為高塔及建物樓頂，用來提供基本的 5G 戶外訊號涵蓋以及有限度的室內訊號涵蓋。小型基地

臺則用來提高基地臺的布署密度，填補大型基地臺訊號死角與加強室內的訊號涵蓋以及提升熱點的系統容量。

3.7 SMO (Service Management and Orchestration)

提供網路設施的管理服務，其管理介面及管理內容包括故障、組態、歸責、效能及安全管理(Fault Configuration Accounting Performance Security, FCAPS)，雲平台(O-Cloud)的資源及負載管理以及 O-RU 的管理。

3.8 Non-RT RIC (Non-Real Time Radio Access Network Intelligent Controller)

位於 SMO 內包括資料分析、訓練機器學習(Machine Learning, ML)模型、提供額外資訊(Enrichment Information)、設定方針(Policy)等功能。

3.9 Near-RT RIC (Near Real Time Radio Access Network Intelligent Controller)

位於無線接取網路(Radio Access Network, RAN)內，接收與分析來自無線接取網路(RAN)的即時資訊，結合 Non-RT RIC 提供的額外資訊，並利用 Non-RT RIC 布署的機器學習模型，監控或預測用戶連線狀況的變化。

3.10 O-CU (O-RAN Central Unit)

是一個網路元件負責 Open RAN 基地臺中，無線資源控制(Radio Resource Control, RRC)與服務數據適配協定(Service Data Adaptation Protocol, SDAP)以及封包數據匯聚協定(Packet Data Convergence Protocol, PDCP)等網路功能[16]。

3.11 O-DU (O-RAN Distributed Unit)

是一個網路元件負責 Open RAN 基地臺中，無線鏈路控制(Radio Link Control, RLC)與媒體存取控制(Media Access Control, MAC)以及上層實體層(Upper Physical layer, Upper-PHY)等網路功能[16]。

3.12 O-RU (O-RAN Radio Unit)

是一個網路元件負責 Open RAN 基地臺中，下層實體層(Lower Physical layer, Lower-PHY)以及射頻(Radio Frequency, RF)信號處理等網路功能[16]。

3.13 5GC (5G Core Network)

乃指 3GPP 5G 系統中與 5G 接取網路相連，且透過控制平面(Control Plane)與用戶平面(User Plane)分割技術，實現以服務為基礎(Service Based Architecture, SBA)之網路虛擬化(Network Virtualization)架構(2)。5GC 透過下一代應用協定(NGAP)與通用封包無線服務隧道協定-用戶平面(GTP-U)連接 O-CU。

3.14 存取與移動管理功能 (Access and Mobility Management Function, AMF)

負責用戶設備(UE)進入行動網路的註冊管理與身分驗證、非接取層(Non Access Stratum, NAS)信令(signaling)的加密與完整性保護、緊急電話(Emergency Call)的定位服務管理、用戶設備移動換手(handover)管理以及合法監聽(Lawful Interception, LI)等功能。

3.15 連結管理功能 (Session Management Function, SMF)

負責用戶設備(UE)連結建立/修改/釋放之管理、動態主機組態協定(Dynamic Host Configuration Protocol, DHCP)功能與 IP 地址分配管理、位址解析協定(Address Resolution Protocol, ARP)代理管理、配置用戶平面功能(UPF)的流量控制、連結和服務連續性

(Session and Service Continuity, SSC)模式、收集電信營運商收費資訊、用戶平面安全策略管理以及合法監聽等功能。

3.16 用戶平面功能 (User Plane Function, UPF)

負責用戶設備(UE)上網連線、資料封包檢查與路由和轉發、用戶平面的流量監控與服務品質(QoS)管理、連接外部資料網路(DN)的管理、用戶平面部分策略規則管理以及合法監聽等功能。

3.17 資料網路 (Data Network, DN)

是一個讓用戶設備 (UE) 識別網路服務供應商服務，實現存取網際網路服務或第三方服務的網路元件。

3.18 服務數據適配協定 (Service Data Adaptation Protocol, SDAP)

主要功能就是對無線電承載(Data Radio Bearer, DRB)與傳輸資料的服務品質(QoS)間進行映射。由於用戶設備(UE)與 O-CU 間透過下一代無線接取介面(NG RAN Air Interface)在封包資料匯聚通訊協定(PDCP)使用資料無線電承載(DRB)傳輸資料，而 O-CU 與 5GC 間則是透過基於服務品質(QoS)為基礎的 N3 介面傳輸資料，因此需要透過服務數據適配協定(SDAP)層將資料無線電承載(DRB)與對應的服務品質(QoS)作映射。

3.19 無線電資源控制 (Radio Resource Control, RRC)

無線電資源控制是做無線電資源分配與管理，主要提供非接取層(NAS)系統資訊廣播；建立、維護和釋放用戶設備(UE)與 O-CU 之間的無線電資源控制連線；臨時標識的分配和用於無線電資源控制連接信令的無線電承載(RB)配置；金鑰安全管理的功能；建立、配置、維護和釋放點對點的無線電承載(RB)；移動性功能包括用戶設備(UE)測量回報和選擇連線的 O-CU；服務品質(QoS)管理功能；非接取層(NAS)消息的傳輸等。

3.20 封包資料匯聚通訊協定 (Packet Data Convergence Protocol, PDCP)

主要負責網際網路協定(Internet Protocol, IP)表頭壓縮與解壓縮，數據與信令的加密及信令的初始化保護等功能。其中在控制平面部分必須啟用加密和初始保護，而在用戶平面部分必須啟用選強健標頭壓縮(Robust Header Compression, ROHC)功能，用戶平面的數據加密為可選擇的功能，其中用戶平面的數據包含應用層信令，如會談初始協定(Session Initiation Protocol, SIP)或即時傳輸控制協定(Real-time Transport Control Protocol, RTCP)等。

3.21 非接取層 (Non Access Stratum, NAS)

非接取層為用戶設備(UE)與 5GC 間控制信令的機制，提供移動性管理、無線電承載(Radio Bearer, RB)設定、用戶的入網與認證等網路功能。

3.22 rApps 應用程式

位於 Non-RT RIC 並提供 Non-RT RIC 的資料分析與訓練機器學習(ML)模型功能，是從 SMO 獲取無線接取網路(Radio Access Network, RAN)相關資料以及從應用服務端獲取用戶相關資料。並應用機器學習方法，針對個別目的，以離線(off-line)識別訓練或預測模型方式，將機器學習模型布署於 Near-RT RIC，可因應流量與環境的變化，主動並提前調整網路資源配置。

3.23 xApps 應用程式

位於 Near-RT RIC 並利用機器學習模型，監控或預測用戶連線狀況的變化，一旦發現可能達不到 Non-RT RIC 設定的方針，則需對無線接取網路(RAN)參數進行調整，例如調整資源分配、傳輸率、傳輸優先性、切換連接點、換手(handover)…等方式，使各用戶可繼續維持既定的方針目標。

3.24 下一代應用協定 (NG Application Protocol, NGAP)

為 O-CU 和存取與移動管理功能(AMF)間處理 N2 介面之相關信令與程序(3)，該協定包含用戶設備(UE)設定更新和設定內容轉移、連線管理閒置(CM Idle)和連線管理連線(CM Connected)之用戶設備狀態管理、PDU 會話資源管理、用戶設備移動換手(handover)管理以及轉送上下行鏈路之非接取層(NAS)信令。

3.25 通用封包無線服務隧道協定-用戶平面 (GPRS Tunnel Protocol- User Plane, GTP-U)

是一個以網際網路協定(Internet Protocol, IP)為基礎的簡單穿隧協定(4)，該協定允許用戶設備(UE)與用戶平面功能(UPF)間建立隧道連線，使得用戶設備可以使用任意形式的封包協定(如 IPv4、IPv6 或 PPP 等協定)透過 5GC 傳送至資料網路(DN)。

3.26 Xn 應用協定 (Xn Application Protocol, XnAP)

為兩台 O-CU 間處理 Xn 介面之相關信令與程序(5)，該協定包含用戶設備(UE)設定更新和設定內容轉移與用戶設備移動換手(handover)管理等。

3.27 F1 應用協定 (F1 Application Protocol, F1AP)

為 O-CU 與 O-DU 間處理 F1-C 介面之相關信令與程序(6)，該協定包含傳送用戶設備(UE)的無線資源控制(Radio Resource Control, RRC)信令等資訊。

3.28 E2 應用協定 (E2 Application Protocol, E2AP)

為 Near-RT RIC 與 O-CU 與 O-DU 間處理 E2 介面之相關信令與程序(8)。

3.29 A1 應用協定 (A1 Application Protocol, A1AP)

為 Non-RT RIC 與 Near-RT RIC 間，處理 A1 介面之相關信令與程序(9)。

3.30 O1 介面 (OAM Interface/O1 Interface)

為 SMO 與 Near-RT RIC、O-CU、O-DU 與 O-RU 間，處理故障、組態、歸責、效能及安全管理(Fault Configuration Accounting Performance Security, FCAPS)之相關信令與程序(10)。

3.31 O2 介面 (O2 Interface)

為SMO與雲平台(O-Cloud)間，處理處理故障、組態、歸責、效能及安全管理(Fault Configuration Accounting Performance Security, FCAPS)之相關信令與程序(11)。

3.32 Open FH 介面 (Open Fronthaul Interface)

是一個通用的無線電介面標準，定義 O-DU 與 O-RU 間介面的基頻 I/Q 訊號傳輸協定的控制、用戶和同步平面(Control, User and Synchronization Plane, CUS-Plane)以及管理平面(Management Plane, M-Plane)(12)。

3.33 NG-RAN/NR-Uu 介面 (Next Generation Radio Access Network, NG-RAN/NR-Uu Interface)

為用戶設備 (UE) 和 O-RU 間之 5G 無線網路的接取介面，支援增強型行動寬頻通訊 (Enhanced Mobile Broadband, eMBB)、超可靠度和低延遲通訊 (Ultra-reliable and Low Latency Communications, URLLC)、增強型機器類通訊 (Enhanced Machine-Type Communications, eMTC)以及蜂巢式車聯網通訊 (Cellular Vehicle-to-Everything, C-V2X)等服務。

3.34 5gcuSIM (5GC+CU Simuator)

為具備 O-CU 並與待測 O-DU 相同 F1-C 介面連線之模擬裝置，能夠讓待測 O-DU 透過 F1 應用協定(F1AP)與 5gcuSIM 進行註冊，並在檢測過程中能夠透過 F1-C 介面對待測 O-DU 回復用戶設備 (UE) 的無線電資源控制 (RRC) 協定封包，並透過 F1-U 介面對待測 O-CU 回復用戶設備 (UE) 的用戶平面資料，以驗證 O-DU 的資安功能。

為具備 O-CU 並與待測 Near-RT RIC 相同 E2 介面連線之模擬裝置，能夠讓 5gcuSIM 透過 E2 應用協定(E2AP)與待測 Near-RT RIC 進行註冊，並在檢測過程中能夠透過 E2 介面對待測 Near-RT RIC 發送 E2 應用協定(E2AP)封包，以驗證 Near-RT RIC 的資安功能。

3.35 DuSIM (DU Simuator)

為具備 O-DU 並與待測 O-CU 相同 F1-C 介面連線之模擬裝置，能夠讓 DuSIM 透過 F1 應用協定(F1AP)與待測 O-CU 進行註冊，並在檢測過程中能夠透過 F1-C 介面對待測 O-CU 發送用戶設備 (UE) 的無線電資源控制 (RRC) 協定封包，並透過 F1-U 介面對待測 O-CU 發送用戶設備 (UE) 的用戶平面資料，以驗證 O-CU 的資安功能。

且具備 O-DU 並與待測 Near-RT RIC 相同 E2 介面連線之模擬裝置，能夠讓 DuSIM 透過 E2 應用協定(E2AP)與待測 Near-RT RIC 進行註冊，並在檢測過程中能夠透過 E2 介面對待測 Near-RT RIC 發送 E2 應用協定(E2AP)封包，以驗證 Near-RT RIC 的資安功能。

3.36 RuSIM (RU Simuator)

為具備 O-RU 並與待測 O-DU 相同 Open FH 介面連線之模擬裝置，能夠讓 RuSIM 透過 Open FH-C 介面經由 O-DU 與待測 O-CU 進行註冊，並在檢測過程中能夠透過 Open FH-C 介面經由 O-DU 對待測 O-CU 發送用戶設備 (UE) 的無線電資源控制 (RRC) 協定封包，並透過 Open FH-U 介面經由 O-DU 對待測 O-CU 發送用戶設備 (UE) 的用戶平面資料，以驗證 O-CU 的資安功能。

3.37 RicSIM (Near-RT RIC Simuator)

為具備 Near-RT RIC 並與待測 O-CU 相同 E2 介面連線之模擬裝置，能夠讓待測 O-CU 透過 E2 應用協定(E2AP)與 RicSIM 進行註冊，並在檢測過程中能夠透過 E2 介面對待測 O-CU 發送 E2 應用協定(E2AP)封包，以驗證 O-CU 的資安功能。

具備 Near-RT RIC 並與待測 O-DU 相同 E2 介面連線之模擬裝置，能夠讓待測 O-DU 透過 E2 應用協定(E2AP)與 RicSIM 進行註冊，並在檢測過程中能夠透過 E2 介面對待測 O-DU 發送 E2 應用協定(E2AP)封包，以驗證 O-DU 的資安功能。

具備 Near-RT RIC 並與待測 Non-RT RIC 相同 A1 介面連線之模擬裝置，並在檢測過程中能夠透過 A1 介面對待測 Non-RT RIC 發送 OAuth 2.0 認證訊令，以驗證 Non-RT RIC 的資安功能。

3.38 O-CU 模糊測試器 (O-CU Fuzz Testing Device)

為具備 O-CU 並與待測 O-DU 相同 F1-C 介面連線之模擬裝置，能夠讓待測 O-DU 透過 F1 應用協定(F1AP)與 O-CU 模糊測試器進行註冊，並在檢測過程中能夠透過 F1-C 介面對待測 O-DU 發送非預期的 F1 應用協定封包，用以驗證 O-DU 的強健性。

3.39 O-DU 模糊測試器 (O-DU Fuzz Testing Device)

為具備 O-DU 並與待測 O-CU 相同 F1-C 介面連線之模擬裝置，能夠讓待測 O-CU 透過 F1 應用協定(F1AP)與 O-DU 模糊測試器進行註冊，並在檢測過程中能夠透過 F1-C 介面對待測 O-CU 發送非預期的 F1 應用協定封包，用以驗證 O-CU 的強健性。

3.40 O-RU 模糊測試器 (O-RU Fuzz Testing Device)

為具備 O-RU 並與待測 O-DU 相同開放前傳介面(Open Fronthaul Interface, Open FH)連線之模擬裝置，並在檢測過程中能夠透過開放前傳介面(Open FH)對待測 O-DU 發送非預期的演進版通用公共無線電介面(evolved Common Public Radio Interface, eCPRI)協定封包，亦或常態性乙太網路訊框(generic Ethernet frames)及高精確時間協定(Precision Time Protocol, PTP) announce/sync 信令封包，用以驗證 O-DU 的強健性。

3.41 O-RU 阻斷服務攻擊模擬器 (O-RU DoS Attack Simulator)

為具備 O-RU 並與待測 O-DU 相同開放前傳介面(Open Fronthaul Interface, Open FH)連線之模擬裝置，並在檢測過程中能夠透過開放前傳介面(Open FH)對待測 O-DU 發送非預期的演進版通用公共無線電介面(evolved Common Public Radio Interface, eCPRI)協定封包，亦或常態性乙太網路訊框(generic Ethernet frames)及高精確時間協定(Precision Time Protocol, PTP) announce/sync 信令封包，用以驗證 O-DU 的強健性。

3.42 Near-RT RIC 模糊測試器 (Near-RT RIC Fuzz Testing Device)

為具備 Near-RT RIC 並與待測 Non-RT RIC 相同 A1 介面連線之模擬裝置，並在檢測過程中能夠 A1 介面對待測 Near-RT RIC 的產生超文件傳輸協定(HyperText Transfer Protocol, HTTP)或超文件傳輸安全協定(HyperText Transfer Protocol Secure, HTTPs)的表現層狀態轉換(REpresentational State Transfer, REST)應用介面(APplication Interface, API)信令之非預期訊號攻擊封包。

3.43 Near-RT RIC 阻斷服務攻擊模擬器 (Near-RT RIC DoS Attack Simulator)

為具備 Near-RT RIC 並與待測 Non-RT RIC 相同 A1 介面連線之模擬裝置，並在檢測過程中能夠 A1 介面對於 Non-RT RIC 產生超文件傳輸協定(HyperText Transfer Protocol, HTTP)或超文件傳輸安全協定(HyperText Transfer Protocol Secure, HTTPs)的表現層狀態轉換(REpresentational State Transfer, REST)應用介面(APplication Interface, API)信令之阻斷服務攻擊封包。

3.44 訊息完整性鑑別碼 (Message Authentication Code for Integrity, MAC-I)

亦稱為完整性檢查碼(Integrity Check Value, ICV)，作為確認發送訊息者的身分，以保證訊息的完整性(Integrity)。傳送端一般都利用雜湊函數(Hash Function)計算出一個固定長度的雜湊值，作為一個獨一無二的訊息認證。它的總長度為 4 位元組。

3.45 ISAKMP (Internet Security Association and Key Management Protocol)

指一網際網路安全關聯與金鑰管理協定，為用於在網際網路上進行授權與金鑰交換的架構。ISAKMP 協定定義於 RFC 2408 標準規範文件中，主要功能是建立、修改與刪除『安全關聯』(Security association, SA)，其中包含協議雙方的加密金鑰、認證金鑰、以及各種演算法。

3.46 封裝安全承載 (Encapsulation Security Payload, ESP)

是一個網際網路安全協定(IPSec)，用於封裝安全承載(IPSec ESP)將原網際網路已經修正協定封包(Internet protocol, IP)經過加密後，重新封裝成另一個網際網路協定封包，以達到資料隱密性的功能，同樣也有傳輸模式(Transport mode)與通道模式(Tunnel mode)兩種封包模式。

3.47 網際網路金鑰交換 (Internet Key Exchange, IKE)

是一種建立在奧克利協定(Oakley protocol)與 ISAKMP 上的網路協定。該協定定義於 RFC 2409 標準規範文件中。為了配合 ISAKMP 運作，網際網路金鑰交換採用兩階段的協商方式，第一階段 (Phase I) 協商是建立安全通訊連線；第二階段 (Phase II) 才真正進入鑰匙交換程序。

3.48 營運管理與維護 (Operations, Administration and Maintenance, OAM)

是指根據運營商網路運營的實際需要，通常將網路的管理工作劃分為 3 大類：操作(Operation)、管理(Administration)、維護(Maintenance)。

3.49 商用現成產品 (Commercial-Off-the-Shelf, COTS)

是指事先準備好的一組應用程式軟體或硬體設備，並在市場上販售交易，讓個人或企業組織不需要再為特定的功能撰寫自己的軟體程式或開發相關硬體設備。

3.50 自由及開放原始碼軟體 (Free-Open-Source-Software, FOSS)

是一種可以歸類為既是自由軟體又是開源軟體的電腦軟體。也就是任何人被授權可以自由的使用、複製、研究和以任何方式來改動軟體，且其原始碼是開放和共享，同時鼓勵人們志願改善軟體設計。好處包括降低軟體成本，提高安全性、隱性私和穩定性，並讓用戶自行控制自己的硬體。

4. Open RAN 資安風險評估與需求

依據 3GPP TR 33.926 [12]網路產品類別之威脅和關鍵資產的安全保證規範(Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes)與 O-RAN 資安威脅建模和補救分析(O-RAN Security Threat Modeling and Remediation Analysis)研究報告，從 5G 資安風險分析可以歸納出八種威脅層面的主要威脅，分別為 3GPP 定義的網路介面威脅(Threats Relating to 3GPP-defined Interfaces)、O-RAN 定義的網路介面威脅(Threats Relating to ORAN-defined Interfaces)、識別碼欺騙(Spoofing Identity)、竄改(Tampering)、否認性(Repudiation)、資訊揭露(Information Disclosure)、阻斷服務(Denial of service)以及提高特權(Elevation of Privilege)，其中針對 O-RAN 基地臺風險分析如表 1 所示，O-RAN 元件的威脅分析分別如表 2 所示。

表 1 O-RAN 基地臺風險評估

威脅種類	威脅細節
3GPP 定義的網路介面威脅(Threats Relating to 3GPP-defined Interfaces)	N2 介面威脅
	N3 介面威脅
	Xn-C 介面威脅
	F1-C 介面威脅
	NR-Uu 介面威脅
ORAN 定義的網路介面威脅(Threats Relating to ORAN-defined Interfaces)	O1 介面威脅
	O2 介面威脅
	A1 介面威脅
	E2 介面威脅
	Open FH M-Plane 介面威脅
	Open FH C-Plane 介面威脅
	Open FH S-Plane 介面威脅
識別碼欺騙(Spoofing Identity)	預設帳戶 (Default Accounts)
	弱密碼政策 (Weak Password Policies)
	窺視密碼 (Password Peek)
	直接根存取 (Direct Root Access)
	網際通訊協定欺騙 (IP Spoofing)
	惡意程式 (Malware)
	竊聽 (Eavesdropping)
竄改 (Tampering)	軟體竄改 (Software Tampering)
	所有權檔案誤用(Ownership File Misuse)
	開機竄改 (Boot Tampering)
	日誌竄改 (Log Tampering)

	營運管理與維護流量竄改 (OAM Traffic Tampering)
	檔案寫入權限濫用 (File Write Permissions Abuse)
	用戶通信期竄改 (User Session Tampering)
否認性 (Repudiation)	缺乏用戶活動記錄 (Lack of User Activity Trace)
資訊揭露 (Information Disclosure)	不良金鑰產生 (Poor Key Generation)
	不良金鑰管理 (Poor Key Management)
	弱密碼演算法 (Weak Cryptographic Algorithms)
	不安全資料儲存 (Insecure Data Storage)
	系統指紋 (System Fingerprinting)
	惡意程式 (Malware)
	個人識別資訊違規 (Personal Identification Information Violation)*
	不安全預設組態 (Insecure Default Configuration)
	檔案/目錄讀出權限濫用 (File/Directory Read Permissions Misuse)
	資訊揭露-不安全網路服務 (Insecure Network Services)
	非必要服務 (Unnecessary Services)
	日誌揭露 (Log Disclosure)
	非必要應用 (Unnecessary Applications)
	竊聽 (Eavesdropping)
	缺乏通用網路產品流量隔離導致安全威脅 (Security Threat Caused by Lack of GNP Traffic Isolation)
阻斷服務 (Denial of Service)	被破解/行為異常用戶設備 (Compromised/Misbehaving User Equipment)*
	實作缺陷 (Implementation Flaw)*
	阻斷服務-不安全網路服務 (Insecure Network Services)
	人為錯誤 (Human Error)*
提高特權 (Elevation of Privilege)	授權使用者誤用 (Misuse by Authorized Users)*
	超過特權的程序/服務 (Over-Privileged Processes/Services)
	資料夾寫入權限濫用 (Folder Write Permission Abuse)
	根所屬檔案寫入權限濫用 (Root-Owned File Write Permission Abuse)
	高特權檔案 (High-Privileged Files)
	提高特權-不安全網路服務 (Insecure Network Services)
	透過非必要網路服務提高特權 (Elevation of Privilege via Unnecessary Network Services)

註* 需要透過營運機構之通信系統資通安全維護的「管理面」與「制度面」來避免本威脅

表 2 O-RAN 元件的威脅分析

威脅編號	威脅對象	威脅細節
T-O-RAN-01	全部	入侵缺乏安全設計的 O-RAN 元件
T-O-RAN-02	全部	入侵錯誤或不當配置的 O-RAN 元件
T-O-RAN-03	全部	透過網際網路入侵滲透弱認證與存取控制的 O-RAN 網路

威脅編號	威脅對象	威脅細節
T-O-RAN-04	全部	透過物聯網(Internet of Things, IoT)設備干擾 O-RAN 網路的無線通訊信號
T-O-RAN-05	全部	透過開放前傳介面(Open Front-haul Interface)、O1 介面、O2 介面、A1 介面 和 E2 介面滲透破壞 O-RAN 系統
T-O-RAN-06	全部	入侵滲透不完整或不適當之身分驗證和授權機制的 O-RAN 元件
T-O-RAN-07	全部	入侵破壞 O-RAN 監控機制和日誌檔案的完整性和可用性
T-O-RAN-08	全部	入侵破壞 O-RAN 數據的完整性、機密性和可追溯性
T-O-RAN-09	全部	入侵破壞 O-RAN 元件的完整性和可用性
T-FRHAUL-01	前傳介面	透過 O-RAN 無線電單元(O-RU)或前傳介面(Fronthaul Interface)滲透 O-RAN 分散單元(O-DU)及其他元件
T-MPLANE-01	前傳介面的管理平面(M-Plane)	透過中間人(Man in the Middle, MITM)攔截前傳介面(Fronthaul Interface)的管理平面(M-Plane)的資訊
T-SPLANE-01	前傳介面同步平面(S-Plane)	針對主時鐘(Master Clock)進行阻斷服務(Denial of Service, DoS)攻擊
T-SPLANE-02	前傳介面的同步平面(S-Plane)	針對精確時間協定(Precision Time Protocol, PTP)訊息進行中間人(MITM)攔截與選擇性的隨機延遲攻擊
T-CPLANE-01	前傳介面的控制平面(C-Plane)	發送控制平面(C-Plane)下行(Downlink, DL)與上行(Uplink, UL)的欺騙訊息
T-CPLANE-02	前傳介面的控制平面(C-Plane)	針對 O-RAN 分散單元(O-DU)控制平面(C-Plane)進行阻斷服務(DoS)攻擊
T-UPLANE-01	前傳介面的用戶平面(U-Plane)	透過中間人(MITM)攔截前傳介面用戶平面(U-Plane)的資訊
T-ORU-01	O-RU	透過惡意 O-RAN 無線電單元(Rogue O-RU)發動攻擊
T-NEAR-RT-01	近即時無線接取網路智能控制	可以透過惡意 xApps 應用程式 來取得用戶終端(UE)識別碼、追蹤用戶終端(UE)位置和修改用戶終端(UE)優先權等級
T-NONRTRIC-01	非即時無線接取網路智能控制	滲透非即時無線接取網路智能控制(Non-RT RIC)導致降低服務性能，亦或發動阻斷服務(DoS)攻擊
T-xApp-01	近即時無線接取網路智能控制	利用 xApps 應用程式漏洞和錯誤配置發動攻擊
T-xApp-02	近即時無線接取網路智能控制	無意或惡意 xApps 應用程式的衝突會影響 O-RAN 系統功能，進而導致降低服務性能或阻斷服務(DoS)
T-xApp-03	近即時無線接取網路智能控制	破壞 xApps 應用程式的安全隔離
T-rApp-01	非即時無線接取網路智能控制	透過 rApps 應用程式漏洞和錯誤配置發動攻擊

威脅編號	威脅對象	威脅細節
T-rApp-02	非即時無線接取網路智能控制	繞過身分驗證和授權發動攻擊
T-rApp-03	非即時無線接取網路智能控制	破壞 rApps 應用程式的安全隔離
T-rApp-04	非即時無線接取網路智能控制	無意或惡意 xApps 應用程式的衝突會影響 O-RAN 系統功能，進而導致降低服務性能或阻斷服務(DoS)
T-SMO-01 T-SMO-02	服務管理與編排	透過服務管理與編排(SMO)功能上不正確或缺乏身分驗證的弱點發動攻擊
T-SMO-03	服務管理與編排	對服務管理與編排(SMO)發動過載阻斷服務(DoS)攻擊

5. 資安測試分類與測試環境

本測試規範參考 TAICS TR-0025 v1.0「5G Open RAN 資安研究報告」及 TAICS TS-0035 v2.0「5G 基地臺資安測試規範 v2」與無線接取網路聯盟(O-RAN Alliance)之標準規範，針對 5G 獨立組網 (Standalone, SA)之 Open RAN 系統架構下包含 Non-RT RIC、Near-RT RIC、 O-CU 與 O-DU 及 O-RU 等訂定資安測試規範之實施細節，其檢測面向涵蓋行動通訊安全以及系統與應用服務安全兩大類檢測項目，其中資安需求的章節與本測試規範的章節對應關係列於附錄 A。本測試規範具體明列資安檢測之測試項目、測試條件、測試方法與檢測結果等事項，檢測方式可採用分析工具或自動測試。採用分析工具，可以透過任何封包分析工具(如 Wireshark)協助資安檢測。採用自動測試時，建議對待測物使用包圍測試。「通過」條件為符合測試項目之「測試結果」，不符合測試結果者為「不通過」。如本測試規範檢測項目(含非必測項目)無法實施時，將該項測試項目將該測試標註「不適用」，同時應參考附錄 B 所列議題風險評估表以替代方案降低風險。為了確保待測物的軟體與韌體有取得合法授權，建議送測單位應提供產品軟體清單，包含自行開發、使用第三方開源軟體套件和相對應的版本(version)與授權(license)類型之聲明。

5.1 行動通訊安全

本節參考「3GPP TS 33.523 5G Security Assurance Specification (SCAS); Split gNB product classes」[9]之第 4.2.2 小節與「O-RAN TIFG - O-RAN End-to-end Test」之第 7.1 小節至第 7.2 小節[20]、「O-RAN WG11 - O-RAN Security Test Specifications」[15]以及「5G 基地臺資安測試規範」[1] 之第 5.1 小節制定相對應之行動通訊安全測試項目。

表 3 行動通訊安全檢測項目總表

資安測試規範章節	分類	測試案例	威脅細節
6.1.1	O-CU 無線電資源控制(RRC)封包保護機制	6.1.1.1 無線電資源控制(RRC)信令的完整性保護	NR-Uu 介面威脅用戶通信期竄改
		6.1.1.2 無線電資源控制(RRC)信令完整性檢查失敗	NR-Uu 介面威脅用戶通信期竄改
		6.1.1.3 無線電資源控制(RRC)信令加密	NR-Uu 介面威脅

			竊聽
		6.1.1.4 無線電資源控制(RRC)信令重播攻擊保護	NR-Uu 介面威脅
6.1.2	O-CU 用戶層資料保護機制	6.1.2.1 用戶平面數據資料完整性保護	NR-Uu 介面威脅 用戶通信期竄改
		6.1.2.2 用戶平面完整性檢查失敗	NR-Uu 介面威脅 用戶通信期竄改
		6.1.2.3 用戶平面數據資料加密	NR-Uu 介面威脅 竊聽
		6.1.2.4 用戶平面數據資料重播攻擊保護	NR-Uu 介面威脅
		6.1.2.5 基於連結管理功能(SMF)傳送的安全策略對用戶平面資料進行加密	NR-Uu 介面威脅 竊聽
		6.1.2.6 基於連結管理功能(SMF)傳送的安全策略對用戶平面資料進行完整性保護	NR-Uu 介面威脅 用戶通信期竄改
6.1.3	O-CU 接取層安全演算法檢測	6.1.3.1 O-CU 接取層加密和完整性演算法優先順序	NR-Uu 介面威脅不良金鑰產生
		6.1.3.2 O-CU 金鑰更新-重複使用資料無線電承載識別碼	NR-Uu 介面威脅 不良金鑰管理
		6.1.3.3 O-CU 金鑰更新-雙連結下封包資料匯聚通訊協定(PDCP)計數環繞	NR-Uu 介面威脅 不良金鑰管理
		6.1.3.4 O-CU 金鑰更新-雙連結下重複使用資料無線電承載識別碼	NR-Uu 介面威脅 不良金鑰管理
6.1.4	O-CU 變更安全演算法保護	6.1.4.1 防範 Xn 介面交遞中的降階攻擊	NR-Uu 介面威脅
		6.1.4.2 在 Xn 介面交遞中接取層安全演算法選擇	NR-Uu 介面威脅
6.1.5	O-CU 安全通道檢查	6.1.5.1 控制平面資料在 N2 介面的機密性保護	N2 介面威脅
		6.1.5.2 用戶平面資料在 N3 介面的機密性保護	N3 介面威脅
		6.1.5.3 控制平面資料在 Xn 介面的機密性保護	Xn 介面威脅
		6.1.5.4 控制平面資料在 F1-C 介面的機密性保護	F1-C 介面威脅
		6.1.5.5 用戶平面資料在 F1-U 介面的機密性保護	F1-U 介面威脅
		6.1.5.6 控制平面資料在 E2 介面的機密性保護	E2 介面威脅
		6.1.5.7 控制平面資料在 N2 介面的完整性保護	N2 介面威脅 用戶通信期竄改
		6.1.5.8 用戶平面資料在 N3 介面的完整性保護	N3 介面威脅 用戶通信期竄改
		6.1.5.9 控制平面資料在 Xn 介面的完整性	Xn 介面威脅

		保護	用戶通信期竄改
		6.1.5.10 控制平面資料在 F1-C 介面的完整性保護	F1-C 介面威脅 用戶通信期竄改
		6.1.5.11 用戶平面資料在 F1-U 介面的完整性保護	F1-U 介面威脅 用戶通信期竄改
		6.1.5.12 用戶平面資料在 E2 介面的完整性保護	E2 介面威脅 用戶通信期竄改
6.1.6	O-CU 介面功能安全性檢查	6.1.6.1 通用封包無線服務隧道協定-用戶平面(GTP-U)之過濾功能測試	N3 介面威脅 Xn 介面威脅
		6.1.6.2 N2 介面的模糊測試(非必測項目)	N2 介面威脅
		6.1.6.3 N3 介面的模糊測試(非必測項目)	N3 介面威脅
		6.1.6.4 Xn-C 介面的模糊測試(非必測項目)	Xn-C 介面威脅
		6.1.6.5 F1-C 介面的模糊測試(非必測項目)	F1-C 介面威脅
6.1.7	O-DU 安全通道檢查	6.1.7.1 控制平面資料在 F1-C 介面的機密性保護	F1-C 介面威脅
		6.1.7.2 用戶平面資料在 F1-U 介面的機密性保護	F1-U 介面威脅
		6.1.7.3 控制平面資料在 E2 介面的機密性保護	E2 介面威脅
		6.1.7.4 控制平面資料在 F1-C 介面的完整性保護	F1-C 介面威脅 用戶通信期竄改
		6.1.7.5 用戶平面資料在 F1-U 介面的完整性保護	F1-U 介面威脅 用戶通信期竄改
		6.1.7.6 用戶平面資料在 E2 介面的完整性保護	E2 介面威脅 用戶通信期竄改
6.1.8	O-DU 介面功能安全性檢查	6.1.8.1 F1-C 介面的模糊測試(非必測項目)	F1-C 介面威脅
		6.1.8.2 開放前傳介面 C-Plane 模糊測試(非必測項目)	Open FH 介面的 C-Plane 威脅
		6.1.8.3 開放前傳介面 S-Plane 模糊測試(非必測項目)	Open FH 介面的 S-Plane 威脅
		6.1.8.4 開放前傳介面 C-Plane 阻斷服務測試(非必測項目)	Open FH 介面的 C-Plane 威脅
		6.1.8.5 開放前傳介面 S-Plane 阻斷服務測試(非必測項目)	Open FH 介面的 S-Plane 威脅
6.1.9	O-DU 與 O-RU 共同安全通道檢查	6.1.9.1 安全外殼協定(SSH)的安全測試	Fronthaul 介面的 M-Plane 介面威脅
		6.1.9.2 驗證者驗證	Open FH 介面威脅
		6.1.9.3 申請者驗證	Open FH 介面威脅
6.1.10	RIC 安全通道檢查	6.1.10.1 資料包傳送層安全協定(DTLS)的安全測試(使用 IPsec 時無須測試)	F1-C 介面、F1-U 介面與 E2 介面威脅
		6.1.10.2 傳送層安全協定(TLS)的安全測試	A1 介面、O1 介面與 O2 介面威脅

		6.1.10.3 OAuth 2.0 的安全測試	A1 介面威脅
6.1.11	RIC 介面功能安全性檢查	6.1.11.1 A1 介面模糊測試(非必測項目)	A1 介面威脅
		6.1.11.2 A1 介面阻斷服務測試(非必測項目)	A1 介面威脅

5.2 系統與應用服務安全

本節參考「3GPP TS 33.523 5G Security Assurance Specification (SCAS); Split gNB product classes (Release 18)」[9] 之第 4.2.3 小節至第 4.4 小節與「O-RAN TIFG - O-RAN End-to-end Test」之第 7.3 小節 [20]、「O-RAN WG11 - O-RAN Security Test Specifications」[15]以及「5G 基地臺資安測試規範」[1] 之第 5.2 小節制定相對應之行動通訊安全測試項目。

表 4 系統與應用服務安全檢測項目總表

資安測試規範章節	分類	測試案例	威脅細節
6.2.1	資料安全	6.2.1.1 系統功能造成敏感資料外洩	不安全預設組態
		6.2.1.2 韌體造成敏感資料外洩	不安全資料儲存
		6.2.1.3 確保敏感性資料進行加密處理再儲存	不安全資料儲存
6.2.2	應用程式安全	6.2.2.1 網站伺服器不存在常見之網路應用系統安全弱點	網際通訊協定欺騙
		6.2.2.2 系統使用之協定與服務採最小化設計	非必要服務 超過特權的程序/服務 非必要應用
		6.2.2.3 網路傳輸過程使用加密技術確保資料安全	竊聽 營運管理與維護流量竄改 用戶通信期竄改 日誌竄改
		6.2.2.4 網際網路安全協定(IPsec)已知弱點掃描	網際通訊協定欺騙
		6.2.2.5 安全外殼協定(SSH)已知弱點掃描	網際通訊協定欺騙
		6.2.2.6 資料包傳送層安全協定(DTLS)已知弱點掃描(使用 IPsec 時無須測試)	網際通訊協定欺騙
		6.2.2.7 傳送層安全協定(TLS)已知弱點掃描	網際通訊協定欺騙
		6.2.2.8A1 介面已知弱點掃描(非必測	網際通訊協定欺騙

		項目)	
		6.2.2.9 服務列舉	非必要服務 非必要應用
6.2.3	身分鑑別與授權	6.2.3.1 禁止未經認證與授權使用系統各項功能	提高特權-不安全網路服務
		6.2.3.2 每一個帳號至少要有一個身分鑑別因子方可鑑別成功	弱密碼政策
		6.2.3.3 系統預設帳號應可移除或設置停用	預設帳戶
		6.2.3.4 系統應支援與設定不同組合之密碼複雜性規格	弱密碼演算法
		6.2.3.5 密碼變更機制	弱密碼政策
		6.2.3.6 系統應具備暴力及字典攻擊的防護措施	弱密碼政策
		6.2.3.7 密碼顯示遮罩	窺視密碼
		6.2.3.8 密碼連續輸入錯誤處理	不安全預設組態
		6.2.3.9 授權策略	不安全預設組態
		6.2.3.10 O-RAN 基地臺應支援基於角色之存取控制	直接根存取
		6.2.3.11 登出功能是否有效	不安全預設組態
		6.2.3.12 登入之權限控管	不安全預設組態
		6.2.3.13 檔案系統存取權限控管	高特權檔案 根所屬檔案寫入權限濫用 資料夾寫入權限濫用 所有權檔案誤用 檔案寫入權限濫用 檔案/目錄讀出權限濫用
		6.2.3.14 O-RAN 基地臺應支援操作逾時功能	不安全預設組態 阻斷服務-不安全網路服務
		6.2.3.15 暴力破解	預設帳戶 弱密碼政策
		6.2.3.16 未經授權的密碼重置	不安全預設組態
		6.2.3.17 強制密碼政策	弱密碼政策 不安全預設組態
6.2.4	作業系統安全	6.2.4.1 日誌檔不能洩露個人資料	日誌揭露 資訊揭露-不安全網路服務
		6.2.4.2 開機僅可透過合法的韌體	開機竄改
		6.2.4.3 O-RAN 基地臺應具備軟體完整性自我檢測機制	惡意程式 軟體竄改
		6.2.4.4 系統應提供安全事件記錄功能	缺乏用戶活動記錄
		6.2.4.5 系統應提供可將安全事件記	缺乏用戶活動記錄

		錄功能轉移備存至外部系統	
		6.2.4.6 O-RAN 基地臺的安全事件紀錄應有存取控制限制	日誌竄改
		6.2.4.7 確保高權限的系統功能必須經過身分鑑別	透過非必要網路服務提高特權
		6.2.4.8 可卸除儲存媒體禁止啟用自動播放功能	不安全預設組態 惡意程式 軟體竄改
		6.2.4.9 作業系統及網路服務安全	阻斷服務-不安全網路服務
6.2.5	Open RAN 系統安全	6.2.5.1 O-Cloud 虛擬化安全	
		6.2.5.2 分散式阻斷服務攻擊測試	
		6.2.5.3 軟體物料清單簽章	非必要服務 非必要應用
		6.2.5.4 軟體物料清單資料欄位	非必要服務 非必要應用
		6.2.5.5 軟體映像簽章	軟體竄改
		6.2.5.6 軟體簽章驗證	軟體竄改

6. 資安測試規範

本測試規範所需之測試環境與設備需求描述如下，其中測試設備依測試需求分為商用通訊測試設備以及客製化測試設備兩類。

表 5 行動通訊安全測試環境與設備需求

行動安全測試設備	測試設備需求	測試功能
用戶設備	商用通訊測試設備	支援 3GPP REL 15 以上
		支援 5G 獨立組網架構
		支援換手
		透過 NG-RAN 介面完成連線註冊
		透過 NG-RAN 介面發送資料封包
	客製化測試設備	支援 3GPP REL 15 以上
		支援 5G 獨立組網架構
		透過 F1 介面、Open FH 介面或 NG-RAN 介面完成連線註冊
		透過 F1 介面、Open FH 介面或 NG-RAN 介面發送資料封包
		監聽非接取層(NAS)、服務數據適配協定層(SDAP layer)、無線電資源控制層(RRC layer)和封包資料匯聚通訊協定層(PDCP layer)連線資料並存成 log 檔紀錄
		修改支援的加密與完整性演算法，包含 NEA0~3、NIA0~3
		透過 F1 介面、Open FH 介面或 NG-RAN 介面竄改控制平面和用戶平面之封包資料匯聚通訊協定層(PDCP layer)的訊息完整性鑑別碼值
		透過 F1 介面、Open FH 介面或 NG-RAN 介面重播控制平面和用戶平面封包
gNB (Xn 測試用)	商用通訊測試設備	支援 3GPP REL 15 以上
		支援 5G 獨立組網架構
		支援下一代應用協定(NG-AP)和 Xn 應用協定介面(Xn-AP)
		支援 GTP-U 介面
		支援 Xn 介面換手
		監聽 NG-RAN 介面的服務數據適配協定層(SDAP layer)、無線電資源控制層(RRC layer)和封包資料匯聚通訊協定層(PDCP layer)連線資料並存成 log 檔紀錄
		監聽下一代應用協定(NGAP)和 Xn 應用協定(XnAP)連線資料並存成 log 檔紀錄
		設定加密與完整性演算法優先排序，包含 NEA0~3、NIA0~3
		支援用戶平面安全策略
		可支援網際網路安全協定 (IPsec) 用戶端功能
		可支援網際網路金鑰交換第二版 (IKEv2) 協定
		可支援 RFC 8221 網路安全協定封裝安全承載量加密和完整性演

		算法
5GC	商用通訊測試設備	支援 3GPP REL 15 以上
		支援 5G 獨立組網架構
		支援下一代應用協定(NGAP)介面
		支援通用封包無線服務隧道協定-用戶平面(GTP-U)介面
		支援 Xn 介面換手
		監聽下一代應用協定(NGAP)和連線資料並存成 log 檔紀錄
		設定加密與完整性演算法優先排序，包含 NEA0~3、NIA0~3
		支援用戶平面安全策略
際網路安全協定伺服器	商用通訊測試設備	支援網際網路金鑰交換第二版 (IKEv2) 協定
		支援 RFC 8221 網路安全協定封裝安全承載量加密和完整性演算法
基地臺模糊測試裝置	客製化測試設備	支援 3GPP REL 15 以上
		支援 5G 獨立組網架構
		支援 N2 介面和 Xn 介面
		支援 Xn 介面換手
		監聽 N2 介面和 Xn 介面連線資料並存成 log 檔紀錄
		可發送經過修改之 Xn 應用協定(XnAP)封包
用戶平面功能模糊測試裝置	客製化測試設備	支援 3GPP REL 15 以上
		支援 5G 獨立組網架構
		支援 N3 介面
		監聽 N3 介面連線資料並存成 log 檔紀錄
		可發送經過修改 GTP-U 的封包
存取與移動管理功能模糊測試裝置	客製化測試設備	支援 3GPP REL 15 以上
		支援 5G 獨立組網架構
		支援 N2 介面
		監聽 N2 介面連線資料並存成 log 檔紀錄
		可發送經過修改之下一代應用協定(NGAP)封包
O-CU 模糊測試器	客製化測試設備	支援 3GPP REL 15 以上
		支援 5G 獨立組網架構
		支援 F1-C 介面
		監聽 F1-C 介面連線資料並存成 log 檔紀錄
		可發送經過修改之 F1AP 封包
O-DU 模糊測試器	客製化測試設備	支援 3GPP REL 15 以上
		支援 5G 獨立組網架構
		支援 F1-C 介面
		監聽 F1-C 介面連線資料並存成 log 檔紀錄
		可發送經過修改之 F1AP 封包
O-RU 模糊測試器	客製化測試設備	支援 3GPP REL 15 以上
		支援 5G 獨立組網架構
		支援 Open FH 介面
		監聽 Open FH 介面連線資料並存成 log 檔紀錄

		可發送經過修改之 Open FH C-Plane 與 S-Plane 封包
Near-RT RIC 模糊測試器	客製化測試設備	支援 3GPP REL 15 以上
		支援 5G 獨立組網架構
		支援 A1 介面
		監聽 A1 介面連線資料並存成 log 檔紀錄
		可發送經過修改之 A1AP 封包
O-CU 阻斷服務攻擊模擬器	客製化測試設備	支援 3GPP REL 15 以上
		支援 5G 獨立組網架構
		支援 F1-C 介面
		監聽 F1-C 介面連線資料並存成 log 檔紀錄
		可發送經過修改之大量 F1AP 封包
O-DU 阻斷服務攻擊模擬器	客製化測試設備	支援 3GPP REL 15 以上
		支援 5G 獨立組網架構
		支援 F1-C 介面
		監聽 F1-C 介面連線資料並存成 log 檔紀錄
		可發送經過修改之大量 F1AP 封包
O-RU 阻斷服務攻擊模擬器	客製化測試設備	支援 3GPP REL 15 以上
		支援 5G 獨立組網架構
		支援 Open FH 介面
		監聽 Open FH 介面連線資料並存成 log 檔紀錄
		可發送經過修改之大量 Open FH C-Plane 與 S-Plane 封包
Near-RT RIC 阻斷服務攻擊模擬器	客製化測試設備	支援 3GPP REL 15 以上
		支援 5G 獨立組網架構
		支援 A1 介面
		監聽 A1 介面連線資料並存成 log 檔紀錄
		可發送經過修改之大量 A1AP 封包

6.1 行動通訊安全

6.1.1 O-CU 無線電資源控制(RRC)封包保護機制

6.1.1.1 無線電資源控制(RRC)信令完整性保護

(a) 測試依據:

依據 3GPP TS 33.501 [11] 之第 5.3.3 小節與 3GPP TR 33.926 [12] 之第 D.2.2.2 小節，並參考 O-RAN TIFG E2E-Test [20] 之第 7.1 小節以及 3GPP TS 33.523 [9] 之第 4.2.2.1.1 小節和 3GPP TS 33.511 [8] 之第 4.2.2.1.1 小節。

(b) 測試目的:

驗證 O-CU 傳送至用戶設備的 RRC 信令受到完整性保護。

(c) 測試前提：

(1) 用戶設備及 O-CU 可以設定完整性安全演算法。

(2) 用戶設備可以採用 DuSIM 或 RuSIM 之模擬器。

i 當用戶設備為 DuSIM 時，DuSIM、O-CU 及 5GC 間可以成功建立 5G 連線。

ii 當用戶設備為 RuSIM 時，RuSIM、O-DU、O-CU 及 5GC 間可以成功建立 5G 連線。

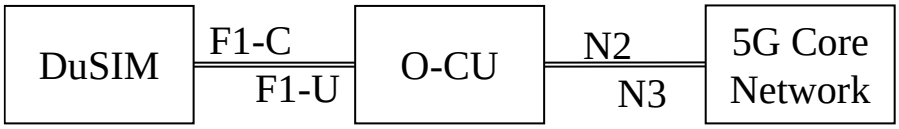
(3) 測試人員可採用分析工具或自動測試。

i 採用工具分析時，需要擷取 F1-C 介面與 N2 介面封包，並分析 F1-C 介面之 RRC 封包的 PDCP 層內容與 N2 介面 NGAP 封包內容。

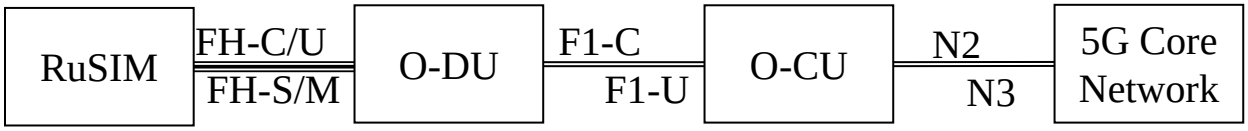
ii 採用自動測試時，需要透過用戶設備分析 RRC 封包的 PDCP 層內容。

(d) 測試佈局：

見圖 2。



(a) 使用 DuSIM 測試



(b) 使用 RuSIM 測試

圖 2 RRC 信令完整性保護測試示意圖

(e) 測試步驟:

(1) 在用戶設備設定支援 NIA1 和 NIA2 完整性安全演算法。

(2) 在 O-CU 端設定 NIA1 完整性安全演算法為最優先選擇。

(3) 採用工具分析時，開始擷取 F1-C 介面與 N2 介面封包。

(4) 確認 O-CU 與 5GC 建立 NGAP 連線，且用戶設備註冊上 5GC。

(5) 採用工具分析時，停止擷取 F1-C 介面與 N2 介面封包。

(6) 採用工具分析時，透過 N2 介面封包的 Initial Context Setup Request 信令中獲取 K_{gNB} 值，並推導出 RRC 完整性金鑰 K_{RRCint}。採用自動測試時，由用戶設備獲取。

(7) 採用工具分析時，透過 F1-C 介面封包，檢查用戶設備和 O-CU 間之 RRC 信令安全驗證程序。採用自動測試時，由用戶設備檢查。

(8) 採用工具分析時，透過 F1-C 介面封包，在完成 RRC 信令安全驗證程序後，確認用戶設備和 O-CU 間之 RRC 信令的 PDCP 層是否帶有訊息完整性鑑別碼。採用自動測試時，由用戶設備確認。

(9) 透過 RRC 完整性金鑰 K_{RRCint} 驗證該完整性鑑別碼的正確性。

(10) 將 O-CU 端設定 NIA2 完整性安全演算法為最優先選擇後，重複(2)~(9)測試步驟。

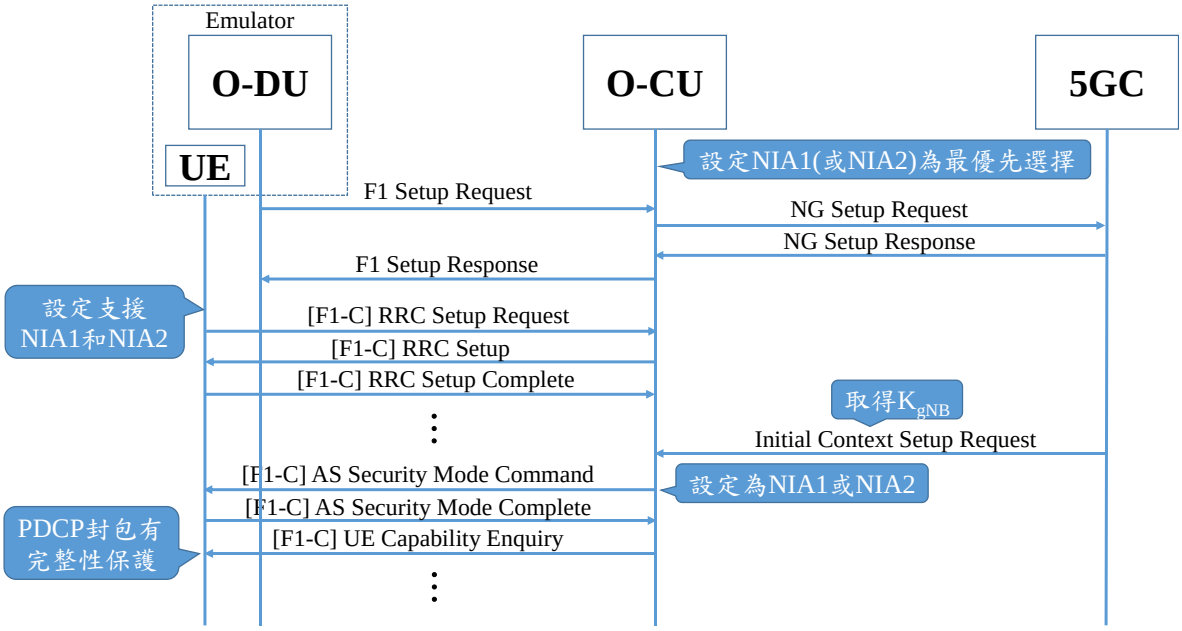


圖 3 RRC 信令的完整性保護測試流程圖

(f) 測試結果:

(1) 根據步驟(7)，O-CU 應傳送帶有完整性演算法 NIA1 或 NIA2 AS Security Mode Command，而用戶設備應回復 AS Security Mode Complete，確保 RRC 信令完整性保護開啟。

(2) 根據步驟(8)與(9)，PDCP 層的訊息應帶有完整性鑑別碼進行完整性保護。用戶設備和 O-CU 會確認完整性鑑別碼為正確後繼續進行 RRC 信令傳輸。

6.1.1.2 無線電資源控制(RRC)信令完整性檢查失敗

(a) 測試依據:

依據 3GPP TS 33.501 [11] 之第 6.5.1 小節與 3GPP TR 33.926 [12] 之第 D.2.2.2 小節，並參考 O-RAN TIFG E2E-Test [20] 之第 7.1 小節以及 3GPP TS 33.523 [9] 之第 4.2.2.1.1 小節和 3GPP TS 33.511 [8] 之第 4.2.2.1.4 小節。

(b) 測試目的:

驗證 O-CU 有正確處置收到完整性檢查失敗的 RRC 信令。

(c) 測試前提:

(1) 用戶設備及 O-CU 可以設定完整性安全演算法。

(2) 用戶設備可以修改 RRC 信令之 PDCP 層的訊息完整性鑑別碼。

(3) 用戶設備可以採用 DuSIM 或 RuSIM 之模擬器。

i. 當用戶設備為 DuSIM 時， DuSIM、O-CU 及 5GC 間可以成功建立 5G 連線。

ii. 當用戶設備為 RuSIM 時， RuSIM、O-DU、O-CU 及 5GC 間可以成功建立 5G 連線。

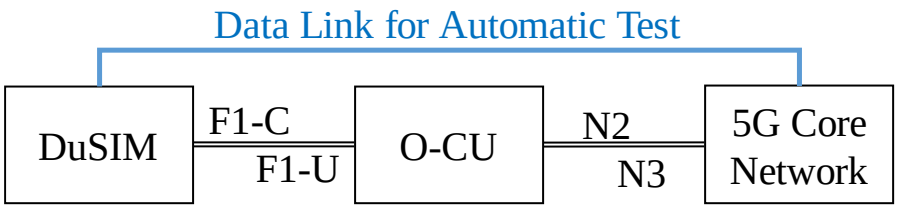
(4) 測試人員可採用分析工具或自動測試。

i. 採用工具分析時，需要擷取 F1-C 介面與 N2 介面封包，並分析 F1-C 介面之 RRC 封包的 PDCP 層內容與 N2 介面 NGAP 封包內容。

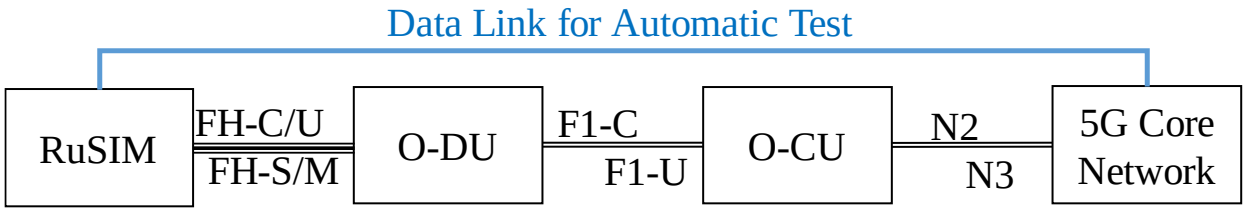
ii. 採用自動測試時，需要透過用戶設備分析 RRC 封包的 PDCP 層內容。如果需要分析 NGAP 封包內容，需要透過 5GC 分析。

(d) 測試佈局：

見圖 4。



(a) 使用 DuSIM 測試



(b) 使用 RuSIM 測試

圖 4 RRC 信令完整性檢查失敗測試示意圖

(e) 測試步驟:

(1) 在用戶設備設定支援 NIA1 和 NIA2 完整性安全演算法。

(2) 在 O-CU 端設定 NIA1 完整性安全演算法為最優先選擇。

(3) 採用工具分析時，開始擷取 F1-C 介面與 N2 介面封包。

(4) 確認 O-CU 與 5GC 建立 NGAP 連線，且用戶設備註冊上 5GC。

(5) 採用工具分析時，從 F1-C 介面封包確認開始進入 RRC 信令安全驗證程序時，用戶設備選擇特定發送給 O-CU 的 RRC 信令封包(如 AS Security Mode Complete 或 UE Capability Information)，該選定之 RRC 信令的 PDCP 層帶有錯誤的訊息完整性鑑別碼或沒夾帶訊息完整性鑑別碼。採用自動測試時，由用戶設備發送。

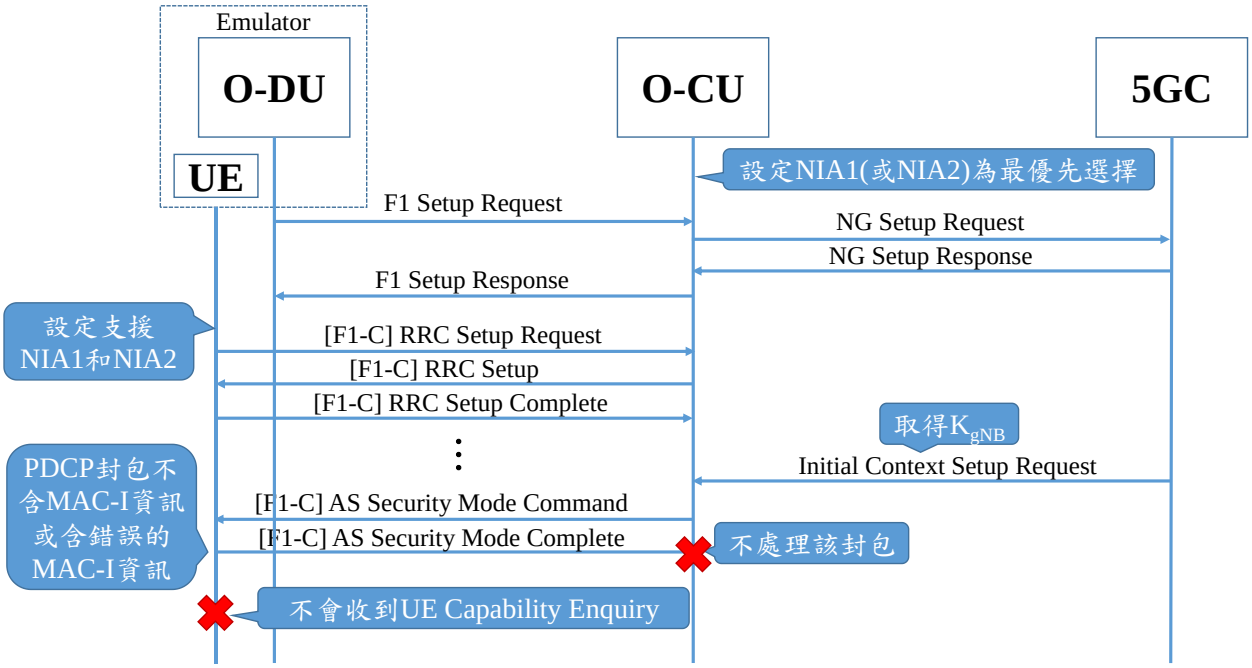
(6) 採用工具分析時，停止擷取 F1-C 介面與 N2 介面封包。

(7) 採用工具分析時，透過 N2 介面封包的 Initial Context Setup Request 信令中獲取 K_{gNB} 值，並推導出完整性金鑰 K_{RRCint}。採用自動測試時，由用戶設備獲取。

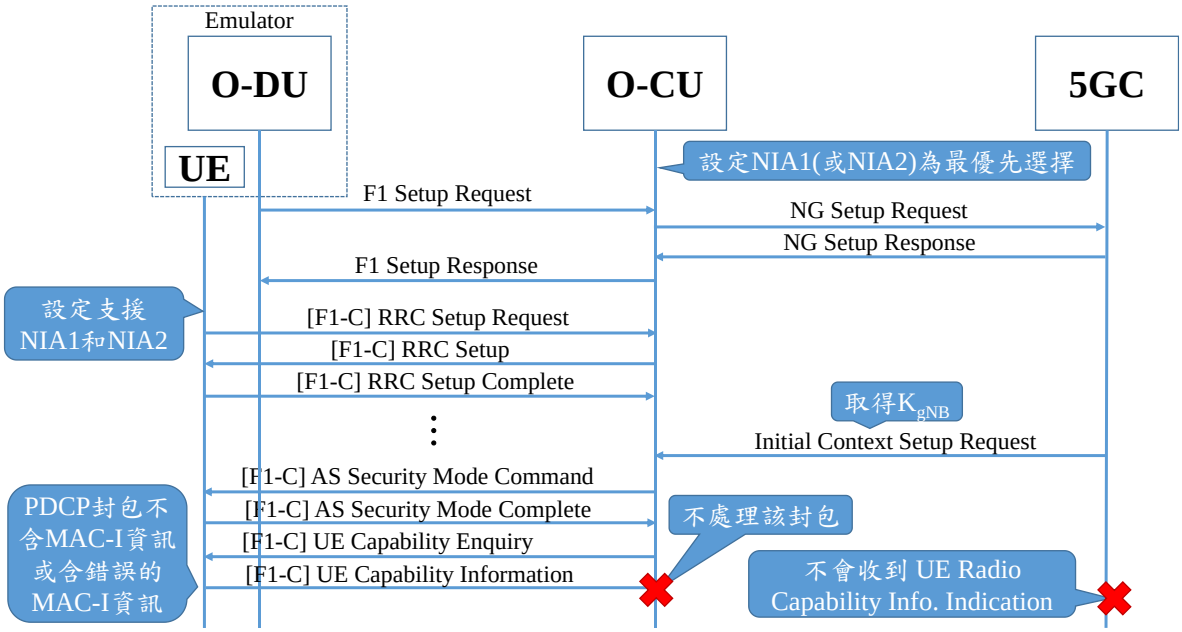
(8) 採用工具分析時，透過 F1-C 介面封包與完整性金鑰 K_{RRCint}，確認 O-CU 是否檢查完整性鑑別碼之正確性。採用自動測試時，由用戶設備檢查。

(9) 如果完整性鑑別碼不正確，O-CU 是否不發送後續的 RRC 信令(如 UE Capability Enquiry) 或不發送後續包含 NAS 的 NGAP 信令(如 UE Radio Capability Info. Indication)。採用自動測試時，由用戶設備檢查 RRC 信令(由 5GC 分析檢查 NGAP 信令)。

(10) 將 O-CU 端設定 NIA2 完整性安全演算法為最優先選擇後，重複(2)~(9)測試步驟。



(a) 用戶設備選擇特定的 RRC 信令封包為 AS Security Mode Complete



(b) 用戶設備選擇特定的 RRC 信令封包為 UE Capability Information

圖 5 RRC 信令完整性檢查失敗測試流程圖

(f) 測試結果:

(1) 根據步驟(8)與(9)，O-CU 檢查來自用戶設備完整性鑑別碼資訊發現是錯誤時，不處理用戶設備回復的 RRC 信令封包(如 AS Security Mode Complete)。

6.1.1.3 無線電資源控制信令加密

(a) 測試依據:

依據 3GPP TS 33.501 [11] 之第 5.3.2 小節與 3GPP TR 33.926 [12] 之第 D.2.2.1 小節，並參考 O-RAN TIFG E2E-Test [20] 之第 7.1 小節以及 3GPP TS 33.512 [9] 之第 4.2.2.1.1 小節和 3GPP TS 33.511 [8] 之第 4.2.2.1.6 小節。

(b) 測試目的:

驗證 O-CU 傳送至用戶設備的 RRC 信令受到機密性保護。

(c) 測試前提:

(1) 用戶設備及 O-CU 可以設定機密性與完整性安全演算法。

(2) 用戶設備可以採用 DuSIM 或 RuSIM 之模擬器。

i. 當用戶設備為 DuSIM 時，DuSIM、O-CU 及 5GC 間可以成功建立 5G 連線。

ii. 當用戶設備為 RuSIM 時，RuSIM、O-DU、O-CU 及 5GC 間可以成功建立 5G 連線。

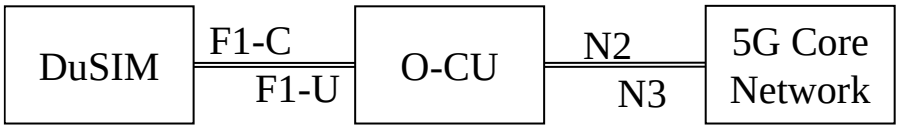
(3) 測試人員可採用分析工具或自動測試。

i. 採用工具分析時，需要擷取 F1-C 介面與 N2 介面封包，並分析 F1-C 介面之 RRC 封包的 PDCP 層內容與 N2 介面 NGAP 封包內容。

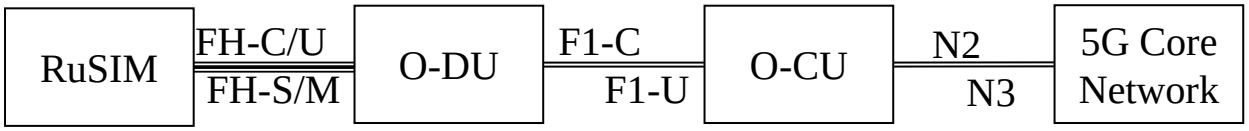
ii. 採用自動測試時，需要透過用戶設備分析 RRC 封包的 PDCP 層內容。

(d) 測試佈局：

見圖 6。



(a) 使用 DuSIM 測試



(b) 使用 RuSIM 測試

圖 6 RRC 信令加密測試示意圖

(e) 測試步驟:

(1) 在用戶設備設定支援 NEA1、NEA2、NIA1、NIA2 機密性和完整性安全演算法。

(2) 在 O-CU 端設定 NEA1、NIA1 機密性和完整性安全演算法為最優先選擇。

(3) 採用工具分析時，開始擷取 F1-C 介面與 N2 介面封包。

(4) 確認 O-CU 與 5GC 建立 NGAP 連線，且用戶設備註冊上 5GC。

(5) 採用工具分析時，停止擷取 F1-C 介面與 N2 介面封包。

(6) 採用工具分析時，透過 N2 介面封包的 Initial Context Setup Request 信令中獲取 K_{gNB} 值，並推導出加密金鑰 K_{RRCenc}。採用自動測試時，由用戶設備獲取 K_{RRCenc} 值。

(7) 採用工具分析時，透過 F1-C 介面封包，檢查用戶設備和 O-CU 之 RRC 信令安全驗證程序。採用自動測試時，由用戶設備檢查 RRC 信令安全驗證程序。

(8) 採用工具分析時，透過 F1-C 介面封包，在完成 RRC 信令安全驗證程序後，確認用戶設備和 O-CU 間 RRC 信令的 PDCP 層訊息是否進行加密保護。採用自動測試時，由用戶設備確認。

(9) 透過 RRC 加密金鑰 K_{RRCenc} 對該 RRC 信令進行解密，並驗證其正確性。

(10) 將 O-CU 端設定 NEA2、NIA2 機密和完整性安全演算法為最優先選擇後，重複(2)~(9)測試步驟。

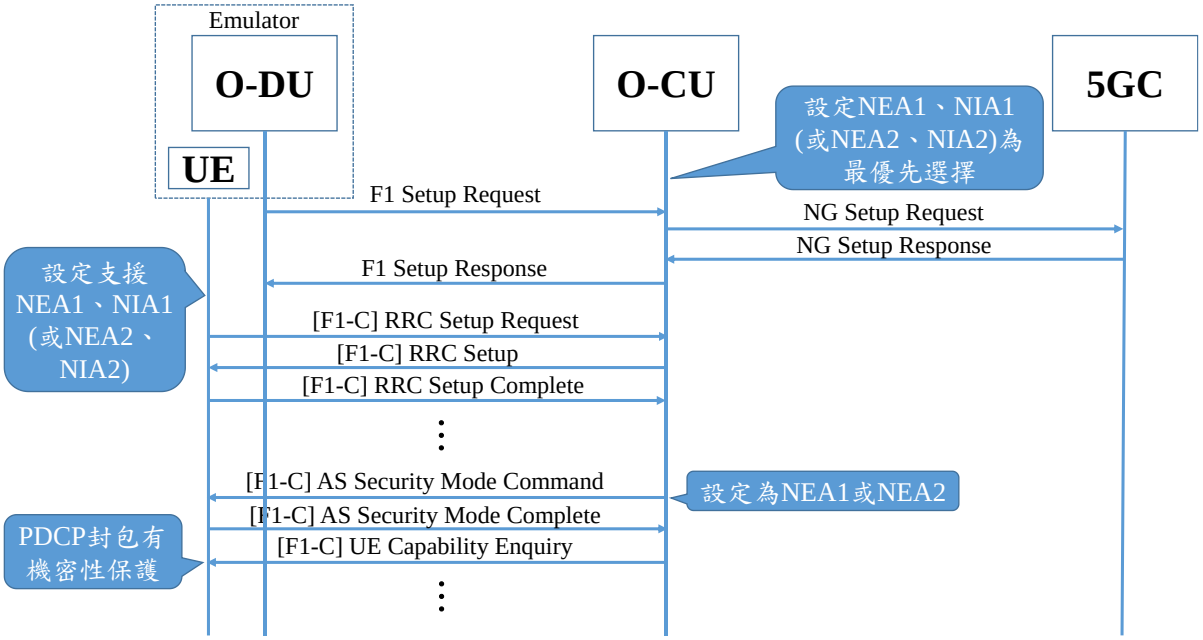


圖 7 RRC 信令加密測試流程圖

(f) 測試結果:

(1) 根據步驟(7)， O-CU 應傳送帶有機密性演算法 NEA1 或 NEA2 AS Security Mode Command，而用戶設備應回復 AS Security Mode Complete，確保 RRC 信令機密性保護開啟。

(2) 根據步驟(8)與(9)，PDCP 層中的訊息會被加密進行機密性保護。用戶設備和 O-CU 因此進行 RRC 信令加密傳輸。

6.1.1.4 無線電資源控制(RRC)信令重播攻擊保護

(a) 測試依據:

依據 3GPP TS 33.501 [11] 之第 5.3.3 小節與 3GPP TR 33.926 [12]之第 D.2.2.2 小節，並參考 O-RAN TIFG E2E-Test [20] 之第 7.1 小節以及 3GPP TS 33.523 [9] 之第 4.2.2.1.1 小節和 3GPP TS 33.511 [8] 之第 4.2.2.1.9 小節。

(b) 測試目的:

驗證 O-CU 接收到的 RRC 制信令受到重播攻擊保護。

(c) 測試前提:

(1) 用戶設備及 O-CU 可以設定完整性安全演算法。

(2) 用戶設備可以重播特定 RRC 信令，其中重播信令的 PDCP 層協定內容(含 PDCP 計數與訊息完整性鑑別碼)需要要和原始信令一樣。

(3) 用戶設備可以採用 DuSIM 或 RuSIM 之模擬器。

i. 當用戶設備為 DuSIM 時，DuSIM、O-CU 及 5GC 間可以成功建立 5G 連線。

ii. 當用戶設備為 RuSIM 時，RuSIM、O-DU、O-CU 及 5GC 間可以成功建立 5G 連線。

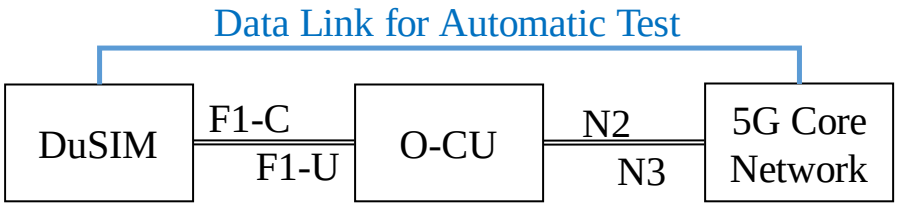
(4) 測試人員可採用分析工具或自動測試。

i. 採用工具分析時，需要擷取 F1-C 介面與 N2 介面封包，並分析 F1-C 介面之 RRC 封包的 PDCP 層內容與 N2 介面 NGAP 封包內容。

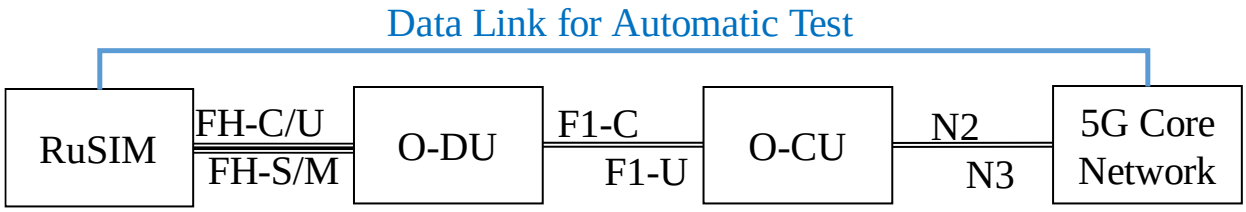
ii. 採用自動測試時，需要透過用戶設備分析 RRC 封包的 PDCP 層內容。如果需要分析 NGAP 封包內容，需要透過 5GC 分析。

(d) 測試佈局：

見圖 8。



(a) 使用 DuSIM 測試



(b) 使用 RuSIM 測試

圖 8 RRC 信令重播攻擊保護測試示意圖

(e) 測試步驟:

(1) 在用戶設備設定支援 NIA1、NIA2 完整性安全演算法。

(2) 在 O-CU 端設定 NIA1 機密性和完整性安全演算法為最優先選擇。

(3) 採用工具分析時，開始擷取 F1-C 介面與 N2 介面封包。

(4) 確認 O-CU 與 5GC 建立 NGAP 連線，且用戶設備註冊上 5GC。

(5) 採用工具分析時，從 F1-C 介面封包確認開始進入 RRC 信令安全驗證程序時，用戶設備選擇特定發送給 O-CU 的 RRC 信令封包(如 AS Security Mode Complete 或 UE Capability Information)進行重播，其中重播信令的 PDCP 層協定內容(含 PDCP 計數與訊息完整性鑑別碼)需要要和原始信令一樣。採用自動測試時，由用戶設備發送。

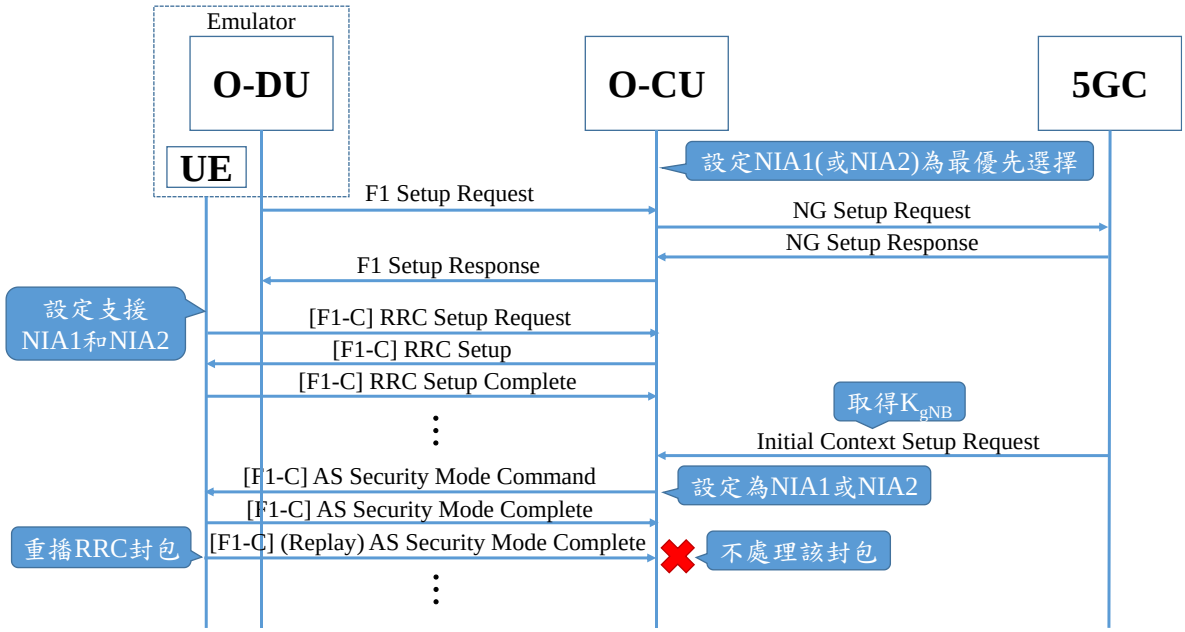
(6) 採用工具分析時，停止擷取 F1-C 介面與 N2 介面封包。

(7) 採用工具分析時，透過 N2 介面封包的 Initial Context Setup Request 信令中獲取 K_{gNB} 值，並推導出完整性金鑰 K_{RRCint}。採用自動測試時，由用戶設備獲取。

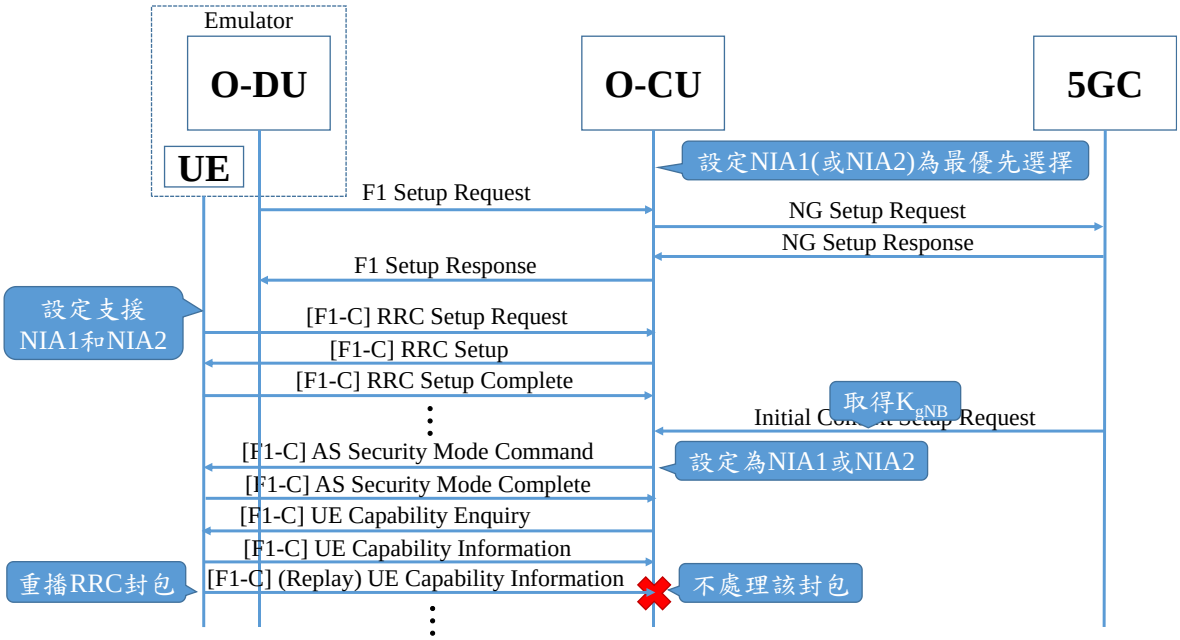
(8) 採用工具分析時，透過 F1-C 介面封包與完整性金鑰 K_{RRCint} 確認重播之 RRC 信令能驗證其完整性鑑別碼和原始信令一樣。採用自動測試時，由用戶設備驗證。

(9) 如果 O-CU 檢查到重播之 RRC 信令的 PDCP 計數重覆，就不發送後續的 RRC 信令(如 UE Capability Enquiry) 或不發送後續包含 NAS 的 NGAP 信令(如 UE Radio Capability Info. Indication)。採用自動測試時，由用戶設備檢查 RRC 信令(用戶由 5GC 分析檢查 NGAP 信令)。

(10) 將 O-CU 端設定 NIA2 機密和完整性安全演算法為最優先選擇後，重複(2)~(9)測試步驟。



(a) 用戶設備選擇特定的 RRC 信令封包為 AS Security Mode Complete



(b) 用戶設備選擇特定的 RRC 信令封包為 UE Capability Information

圖 9 RRC 信令重播攻擊保護測試流程圖

(f) 測試結果:

(1) 根據步驟(9)，O-CU 檢查來自用戶設備 PDCP 計數是重覆時，會丟棄該 RRC 信令封包。

6.1.2 O-CU 用戶層資料保護機制

6.1.2.1 用戶平面數據資料完整性保護

(a) 測試依據:

依據 3GPP TS 33.501 [11] 之第 5.3.3 小節與 3GPP TR 33.926 [12] 之第 D.2.2.4 小節，並參考 O-RAN TIFG E2E-Test [20] 之第 7.1 小節以及 3GPP TS 33.523 [9] 之第 4.2.2.1.1 小節和 3GPP TS 33.511 [8] 之第 4.2.2.1.2 小節。

(b) 測試目的:

驗證 O-CU 傳送至用戶設備的用戶數據資料受到完整性保護。

(c) 測試前提:

(1) 用戶設備及 O-CU 可以設定完整性安全演算法。

(2) SMF 要開啟用戶平面安全策略之用戶平面完整性保護指示。

(3) 用戶設備可以採用 DuSIM 或 RuSIM 之模擬器。

i. 當用戶設備為 DuSIM 時，DuSIM、O-CU 及 5GC 間可以成功建立 5G 連線。

ii. 當用戶設備為 RuSIM 時，RuSIM、O-DU、O-CU 及 5GC 間可以成功建立 5G 連線。

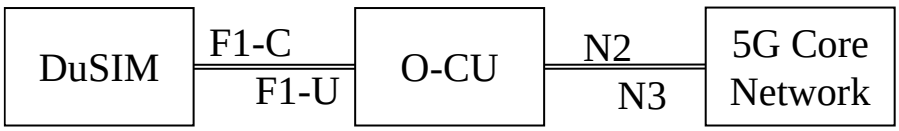
(4) 測試人員可採用分析工具或自動測試。

i. 採用工具分析時，需要擷取 F1-C 介面與 F1-U 介面及 N2 介面封包，並分析 F1-C 介面與 F1-U 介面之 RRC 封包與 GTP-U 封包的 PDCP 層內容，以及分析 N2 介面 NGAP 封包內容。

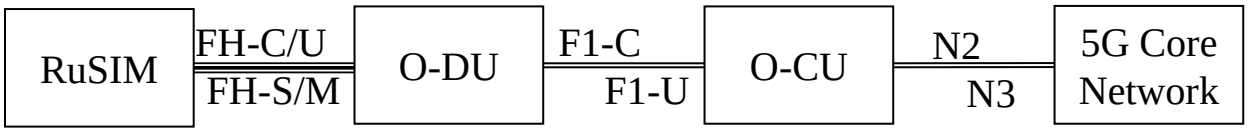
ii. 採用自動測試時，需要透過用戶設備分析 RRC 封包與 GTP-U 封包的 PDCP 層內容。

(d) 測試佈局：

見圖 10。



(a) 使用 DuSIM 測試



(b) 使用 RuSIM 測試

圖 10 用戶數據資料完整性保護測試示意圖

(e) 測試步驟:

(1) 在用戶設備端設定支援 NIA1 和 NIA2 完整性安全演算法。

(2) 在 O-CU 端設定 NIA1 完整性安全演算法為最優先選擇。

(3) 採用工具分析時，開始擷取 F1-C 介面、F1-U 介面及 N2 介面封包。

(4) 確認 O-CU 與 5GC 建立 NGAP 連線，且用戶設備註冊上 5GC 並收送數據資料。

(5) 採用工具分析時，停止擷取 F1-C 介面、F1-U 介面及 N2 介面封包。

(6) 採用工具分析時，透過 N2 介面封包的 Initial Context Setup Request 信令中獲取 K_{gNB} 值，並推導出用戶平面完整性金鑰 K_{UPint}。採用自動測試時，由用戶設備獲取。

(7) 採用工具分析時，透過 F1-C 介面封包，確認用戶設備和 O-CU 完成 RRC 信令安全驗證程序。採用自動測試時，由用戶設備確認。

(8) 採用工具分析時，透過 F1-C 介面封包，確認用戶設備和 O-CU 透過 RRC Reconfiguration 完成用戶平面安全驗證程序。採用自動測試時，由用戶設備確認。

(9) 採用工具分析時，透過 F1-U 介面封包，確認用戶設備和 O-CU 間之用戶平面封包的 PDCP 層訊息帶有完整性鑑別碼。採用自動測試時，由用戶設備確認。

(10) 透過用戶平面完整性金鑰 K_{UPint} 驗證該完整性鑑別碼。

(11) 將 O-CU 端設定 NIA2 完整性安全演算法為最優先選擇後，重複(2)~(10)測試步驟。

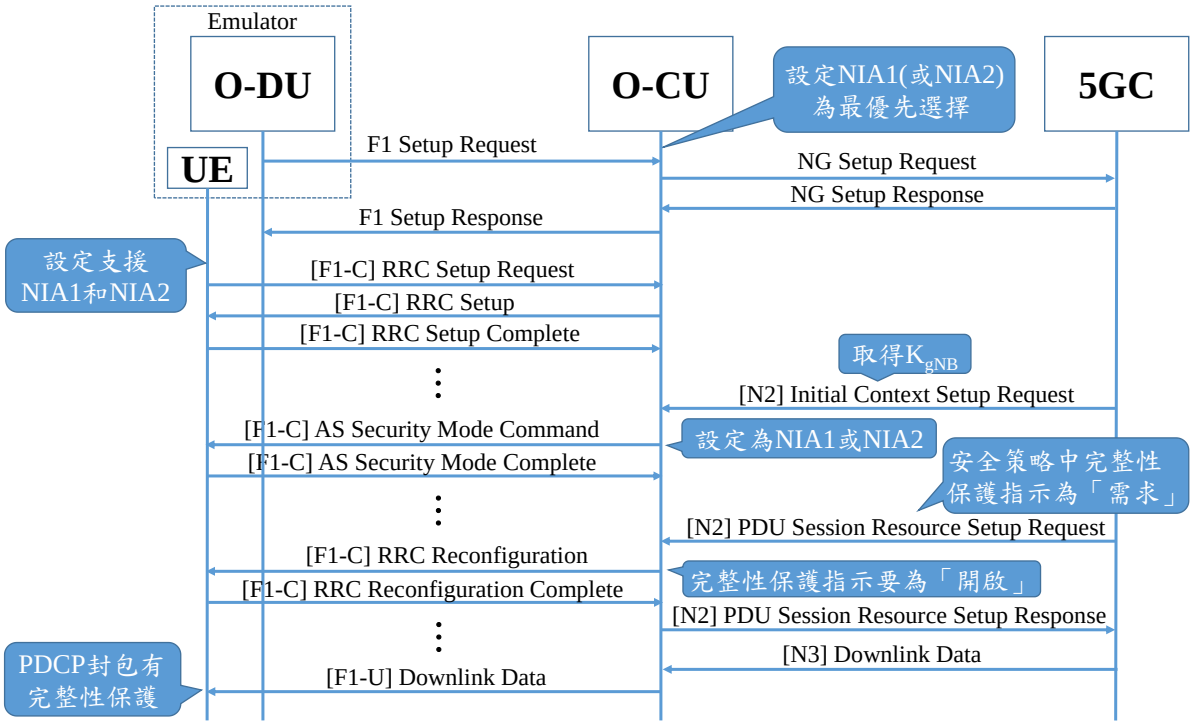


圖 11 用戶數據資料完整性保護測試流程圖

(f) 測試結果:

(1) 根據步驟(8)， O-CU 傳送的 RRC Reconfiguration 中的完整性保護指示要為「開啟」，並且用戶設備回應 RRC Reconfiguration Complete。

(2) 根據步驟(9)與(10)，PDCP 層的訊息應帶有完整性鑑別碼進行完整性保護。用戶設備和 O-CU 會確認完整性鑑別碼為正確後繼續進行用戶平面封包傳輸。

6.1.2.2 用戶平面完整性檢查失敗

(a) 測試依據:

依據 3GPP TS 33.501 [11] 之第 6.6.4 小節與 3GPP TR 33.926 [12] 之第 D.2.2.4 小節，並參考 O-RAN TIFG E2E-Test [20] 之第 7.1 小節以及 3GPP TS 33.523 [9] 之第 4.2.2.1.1 小節和 3GPP TS 33.511 [8] 之第 4.2.2.1.5 小節。

(b) 測試目的:

驗證 O-CU 有正確處置收到完整性檢查失敗的用戶平面資料。

(c) 測試前提:

(1) 用戶設備及 O-CU 可以設定完整性安全演算法。

(2) SMF 要開啟用戶平面安全策略之用戶平面完整性保護指示。

(3) 用戶設備可以修改用戶平面封包之 PDCP 層的訊息完整性鑑別碼。

(4) 用戶設備可以採用 DuSIM 或 RuSIM 之模擬器。

i. 當用戶設備為 DuSIM 時，DuSIM、O-CU 及 5GC 間可以成功建立 5G 連線。

ii. 當用戶設備為 RuSIM 時，RuSIM、O-DU、O-CU 及 5GC 間可以成功建立 5G 連線。

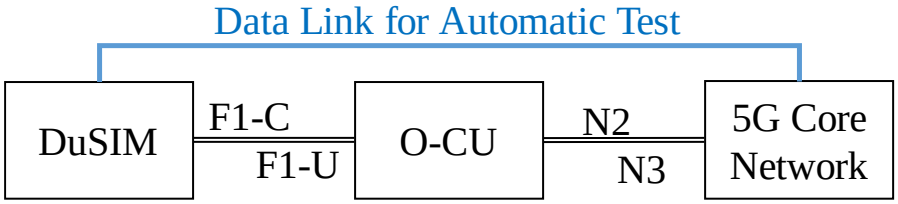
(5) 測試人員可採用分析工具或自動測試。

i. 採用工具分析時，需要擷取 F1-C 介面、F1-U 介面與 N2 介面及 N3 介面封包，並分析 F1-C 介面與 F1-U 介面之 RRC 封包與 GTP-U 封包的 PDCP 層內容，以及分析 N2 介面 NGAP 封包與 N3 介面 GTP-U 封包內容。

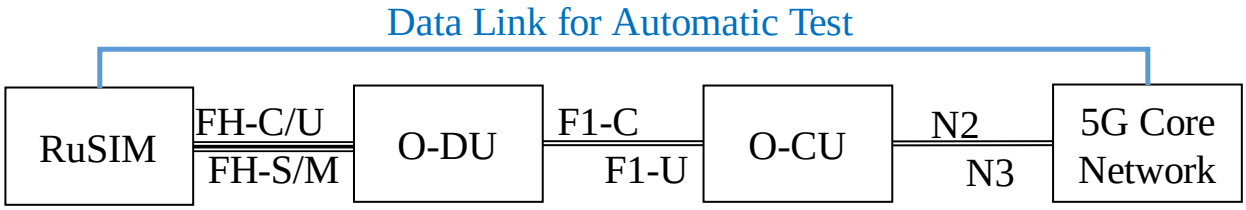
ii. 採用自動測試時，需要透過用戶設備直接分析 RRC 封包與 GTP-U 封包的 PDCP 層內容，且需要透過 5GC 分析 N3 介面的 GTP-U 封包內容。

(d) 測試佈局：

見圖 12。



(a) 使用 DuSIM 測試



(b) 使用 RuSIM 測試

圖 12 用戶平面完整性檢查失敗測試示意圖

(e) 測試步驟:

(1) 在用戶設備端設定支援 NIA1 和 NIA2 完整性安全演算法。

(2) 在 O-CU 端設定 NIA1 完整性安全演算法為最優先選擇。

(3) 採用工具分析時，開始擷取 F1-C 介面、F1-U 介面、N2 介面及 N3 介面封包。

(4) 確認 O-CU 與 5GC 建立 NGAP 連線，且用戶設備註冊上 5GC 並傳送數據資料。

(5) 採用工具分析時，從 F1-C 介面封包確認已經完成 RRC Reconfiguration Complete 時，用戶設備選擇特定發送給 O-CU 的用戶平面封包，該選定之用戶平面封包的 PDCP 層帶有錯誤的訊息完整性鑑別碼或沒夾帶訊息完整性鑑別碼。採用自動測試時，由用戶設備發送。

(6) 採用工具分析時，停止擷取 F1-C 介面、F1-U 介面、N2 介面及 N3 介面封包。

(7) 採用工具分析時，透過 N2 介面封包的 Initial Context Setup Request 信令中獲取 K_{gNB} 值，並推導出用戶平面完整性金鑰 K_{UPint}。採用自動測試時，由用戶設備，由用戶設備獲取。

(8) 採用工具分析時，透過 F1-U 介面封包與用戶平面完整性金鑰 K_{UPint}，確認 O-CU 是否檢查完整性鑑別碼之正確性。採用自動測試時，由用戶設備確認。

(9) 採用工具分析時，如果完整性鑑別碼不正確，透過 N3 介面封包，確認 O-CU 是否不轉送該 F1-U 介面的用戶平面封包到 N3 介面。採用自動測試時，由 5GC 確認。

(10) 將 O-CU 端設定 NIA2 完整性安全演算法為最優先選擇後，重複(2)~(9)測試步驟。

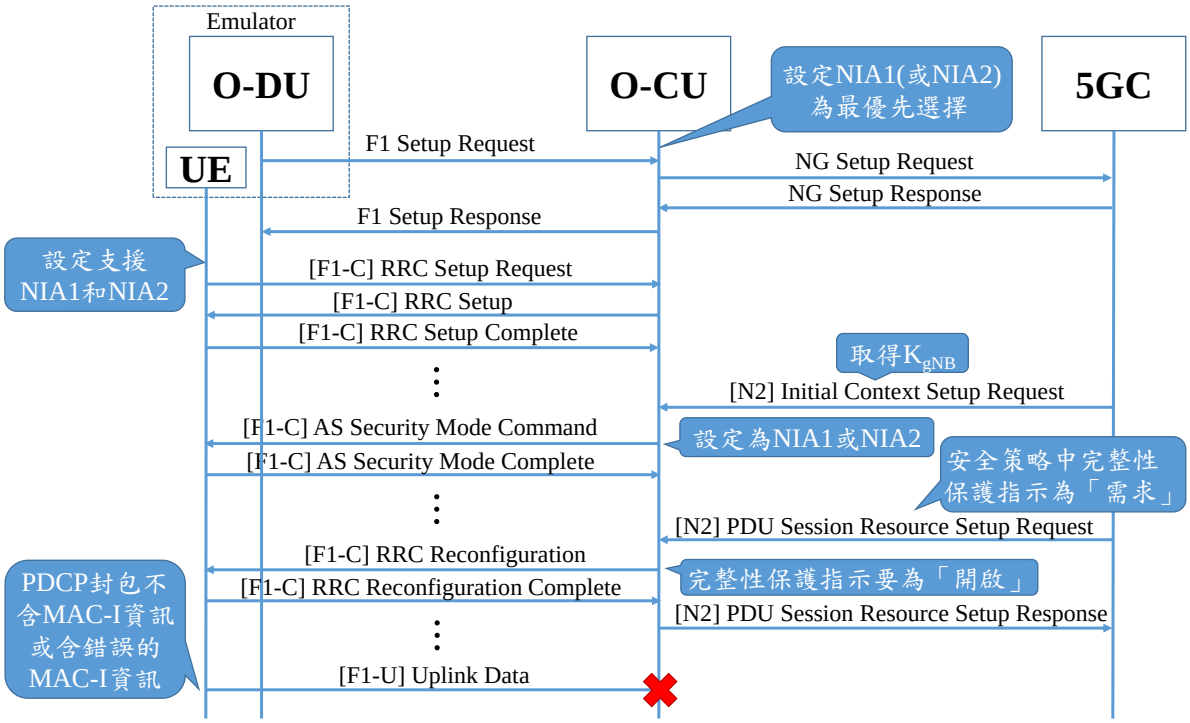


圖 13 用戶平面完整性檢查失敗測試流程圖

(f) 測試結果:

(1) 根據步驟(8)與(9)，O-CU 檢查來自用戶設備完整性鑑別碼資訊發現是錯誤時，會丟棄該用戶平面封包。

6.1.2.3 用戶平面數據資料加密

(a) 測試依據:

依據 3GPP TS 33.501 [11] 之第 5.3.2 小節與 3GPP TR 33.926 [12] 之第 D.2.2.3 小節，並參考 O-RAN TIFG E2E-Test [20] 之第 7.1 小節以及 3GPP TS 33.523 [9] 之第 4.2.2.1.1 小節和 3GPP TS 33.511 [8] 之第 4.2.2.1.7 小節。

(b) 測試目的:

驗證 O-CU 傳送至用戶設備的用戶平面資料受到機密性保護。

(c) 測試前提:

(1) 用戶設備及 O-CU 可以設定完整性安全演算法。

(2) SMF 如果要開啟用戶平面安全策略，其用戶平面資料加密保護指示不能設定為「停用」。

(3) 用戶設備可以採用 DuSIM 或 RuSIM 之模擬器。

i. 當用戶設備為 DuSIM 時，DuSIM、O-CU 及 5GC 間可以成功建立 5G 連線。

ii. 當用戶設備為 RuSIM 時，RuSIM、O-DU、O-CU 及 5GC 間可以成功建立 5G 連線。

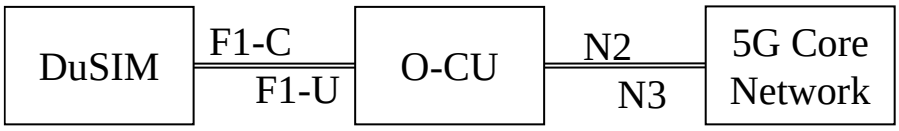
(4) 測試人員可採用分析工具或自動測試。

i. 採用工具分析時，需要擷取 F1-C 介面與 F1-U 介面及 N2 介面封包，並分析 F1-C 介面與 F1-U 介面之 RRC 封包與 GTP-U 封包的 PDCP 層內容，以及分析 N2 介面 NGAP 封包內容。

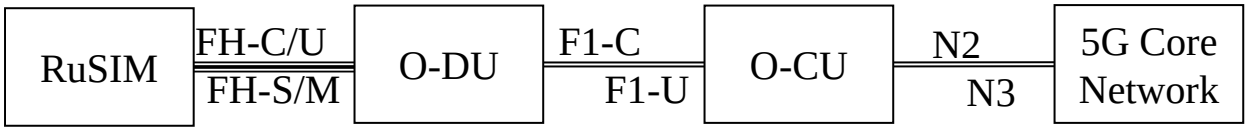
ii. 採用自動測試時，需要透過用戶設備分析 RRC 封包與 GTP-U 封包的 PDCP 層內容。

(d) 測試佈局：

見圖 14。



(a) 使用 DuSIM 測試



(b) 使用 RuSIM 測試

圖 14 用戶平面資料加密測試示意圖

(e) 測試步驟:

(1) 在用戶設備設定支援 NEA1、NEA2、NIA1、NIA2 機密和完整性安全演算法。

(2) 在 O-CU 端設定 NEA1、NIA1 機密和完整性安全演算法為最優先選擇。

(3) 採用工具分析時，開始擷取 F1-C 介面、F1-U 介面及 N2 介面封包。

(4) 確認 O-CU 與 5GC 建立 NGAP 連線，且用戶設備註冊上 5GC 並收送數據資料。

(5) 採用工具分析時，停止擷取 F1-C 介面、F1-U 介面及 N2 介面封包。

(6) 採用工具分析時，透過 N2 介面封包的 Initial Context Setup Request 信令中獲取 K_{gNB} 值，並推導出用戶平面加密金鑰 K_{UPenc}。採用自動測試時，由用戶設備獲取。

(7) 採用工具分析時，透過 F1-C 介面封包，確認用戶設備和 O-CU 完成 RRC 信令安全驗證程序。採用自動測試時，由用戶設備確認。

(8) 採用工具分析時，透過 F1-C 介面封包，確認用戶設備和 O-CU 透過 RRC Reconfiguration 完成用戶平面安全驗證程序。採用自動測試時，由用戶設備確認。

(9) 採用工具分析時，透過 F1-U 介面封包，確認用戶設備和 O-CU 間之用戶平面封包的 PDCP 層訊息被加密保護。採用自動測試時，由用戶設備確認。

(10) 透過用戶平面加密金鑰 K_{UPenc} 對該訊息進行解密，並驗證其正確性。

(11) 將 O-CU 端設定 NEA2、NIA2 機密和完整性安全演算法為最優先選擇後，重複(2)~(11)測試步驟。

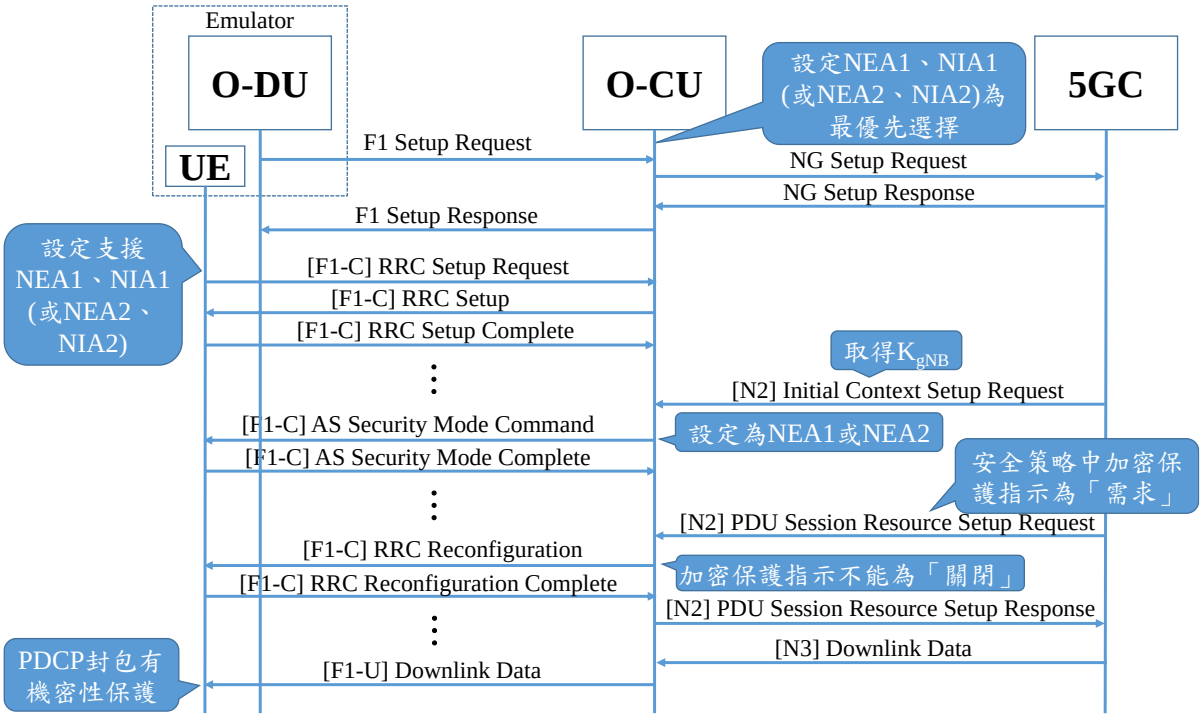


圖 15 用戶平面資料加密測試流程圖

(f) 測試結果:

(1) 根據步驟(8)，O-CU 傳送的 RRC Reconfiguration 中的加密保護指示不能為「關閉」，並且用戶設備回應 RRC Reconfiguration Complete。

(2) 根據步驟(9)與(10)，PDCP 層的訊息應受到加密保護。用戶設備和 O-CU 因此進行用戶平面封包加密傳輸。

6.1.2.4 用戶平面數據資料重播攻擊保護

(a) 測試依據:

依據 3GPP TS 33.501 [11] 之第 5.3.3 小節與 3GPP TR 33.926 [12] 之第 D.2.2.4 小節，並參考 O-RAN TIFG E2E-Test [20] 之第 7.1 小節以及 3GPP TS 33.523 [9] 之第 4.2.2.1.1 小節和 3GPP TS 33.511 [8] 之第 4.2.2.1.8 小節。

(b) 測試目的:

驗證 O-CU 接收到的用戶平面資料受到重播攻擊保護。

(c) 測試前提:

(1) 用戶設備及 O-CU 可以設定完整性安全演算法。

(2) SMF 要開啟用戶平面安全策略之用戶平面完整性保護指示。

(3) 用戶設備可以重播特定用戶平面封包，其中重播封包的 PDCP 層協定內容(含 PDCP 計數與訊息完整性鑑別碼)需要要和原始信令一樣。

(4) 用戶設備可以採用 DuSIM 或 RuSIM 之模擬器。

i. 當用戶設備為 DuSIM 時，DuSIM、O-CU 及 5GC 間可以成功建立 5G 連線。

ii. 當用戶設備為 RuSIM 時，RuSIM、O-DU、O-CU 及 5GC 間可以成功建立 5G 連線。

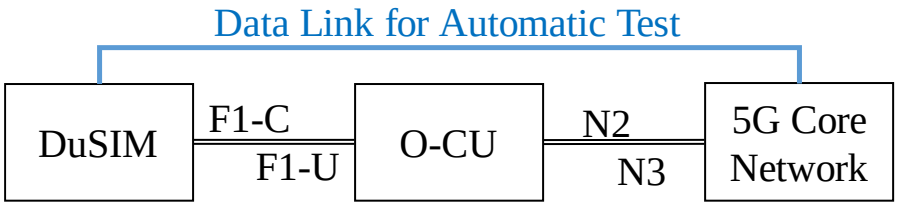
(5) 測試人員可採用分析工具或自動測試。

i. 採用工具分析時，需要擷取 F1-C 介面、F1-U 介面與 N2 介面及 N3 介面封包，並分析 F1-C 介面與 F1-U 介面之 RRC 封包與 GTP-U 封包的 PDCP 層內容，以及分析 N2 介面 NGAP 封包與 N3 介面 GTP-U 封包內容。

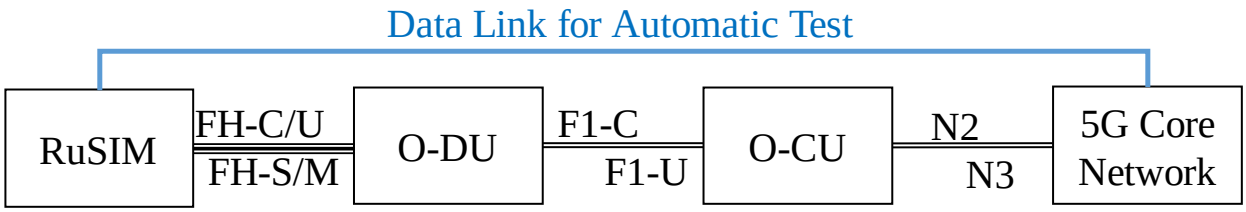
ii. 採用自動測試時，需要透過用戶設備直接分析 RRC 封包與 GTP-U 封包的 PDCP 層內容，且需要透過 5GC 分析 N3 介面的 GTP-U 封包內容。

(d) 測試佈局：

見圖 16。



(a) 使用 DuSIM 測試



(b) 使用 RuSIM 測試

圖 16 用戶數據資料重播攻擊保護測試示意圖

(e) 測試步驟:

(1) 在用戶設備設定支援 NEA1、NEA2、NIA1、NIA2 機密和完整性安全演算法。

(2) 在 O-CU 端設定 NEA1、NIA1 機密和完整性安全演算法為最優先選擇。

(3) 採用工具分析時，開始擷取 F1-C 介面、F1-U 介面、N2 介面及 N3 介面封包。

(4) 確認 O-CU 與 5GC 建立 NGAP 連線，且用戶設備註冊上 5GC 並傳送數據資料。

(5) 採用工具分析時，從 F1-C 介面封包確認已經完成 RRC Reconfiguration Complete 時，用戶設備選擇特定發送給 O-CU 的用戶平面封包進行重播，其中重播封包的 PDCP 層協定內容(含 PDCP 計數與訊息完整性鑑別碼)需要要和原始信令一樣。

(6) 採用工具分析時，停止擷取 F1-C 介面、F1-U 介面、N2 介面及 N3 介面封包。

(7) 採用工具分析時，透過 N2 介面封包的 Initial Context Setup Request 信令中獲取 K_{gNB} 值，並推導出用戶平面完整性金鑰 K_{UPint}。採用自動測試時，由用戶設備獲取。

(8) 採用工具分析時，透過 F1-U 介面封包，透過用戶平面完整性金鑰 K_{UPint} 驗證重播之用戶平面封包，其完整性鑑別碼和原始信令一樣。採用自動測試時，由用戶設備確認。

(9) 如果 O-CU 檢查到重播之用戶平面封包的 PDCP 計數重覆，確認 O-CU 是否不轉送該 F1-U 介面的用戶平面封包到 N3 介面。採用自動測試時，由 5GC 確認。

(10) 將 O-CU 端設定 NEA2、NIA2 機密和完整性安全演算法為最優先選擇後，重複(2)~(9)測試步驟。

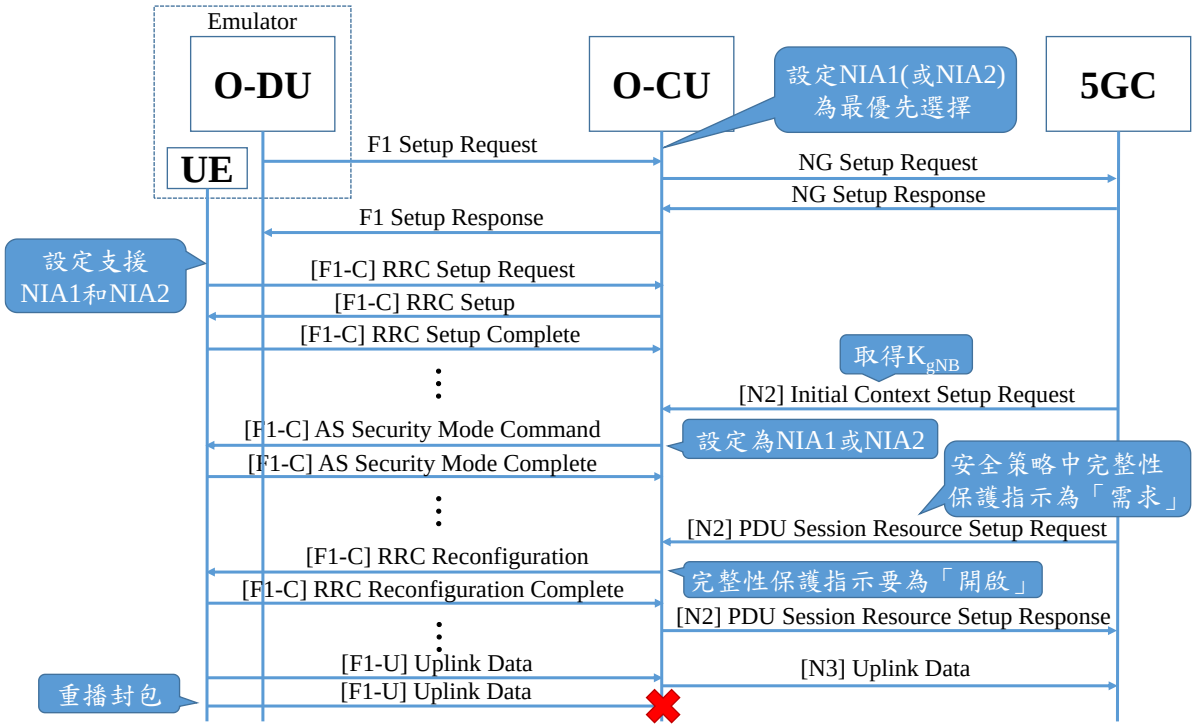


圖 17 用戶數據資料重播攻擊保護測試流程圖

(f) 測試結果:

(1)根據步驟(8)與(9)，O-CU 檢查來自用戶設備 PDCP 計數是重覆時，會丟棄該用戶平面封包。

6.1.2.5 根據連結管理功能(SMF)發送的安全策略對用戶平面資料進行加密

(a) 測試依據:

依據 3GPP TS 33.501 [11] 之第 5.3.3 小節與 3GPP TR 33.926 [12] 之第 D.2.2.2 小節，並參考 O-RAN TIFG E2E-Test [20] 之第 7.1 小節以及 3GPP TS 33.523 [9] 之第 4.2.2.1.1 小節和 3GPP TS 33.511 [8] 之第 4.2.2.1.10 小節。

(b) 測試目的:

驗證用戶平面資料依據 SMF 安全策略受到機密性保護。

(c) 測試前提:

(1)用戶設備及 O-CU 可以設定機密性與完整性安全演算法。

(2)SMF 要開啟用戶平面安全策略之用戶平面機密性保護指示。

(3)用戶設備可以採用 DuSIM 或 RuSIM 之模擬器。

i. 當用戶設備為 DuSIM 時，DuSIM、O-CU 及 5GC 間可以成功建立 5G 連線。

ii. 當用戶設備為 RuSIM 時，RuSIM、O-DU、O-CU 及 5GC 間可以成功建立 5G 連線。

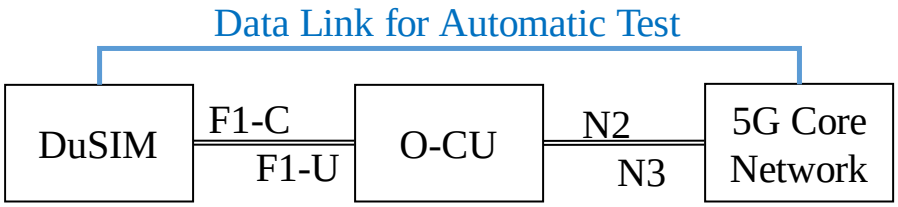
(4)測試人員可採用分析工具或自動測試。

i. 採用工具分析時，需要擷取 F1-C 介面與 F1-U 介面及 N2 介面封包，並分析 F1-C 介面與 F1-U 介面之 RRC 封包與 GTP-U 封包的 PDCP 層內容，以及分析 N2 介面 NGAP 封包內容。

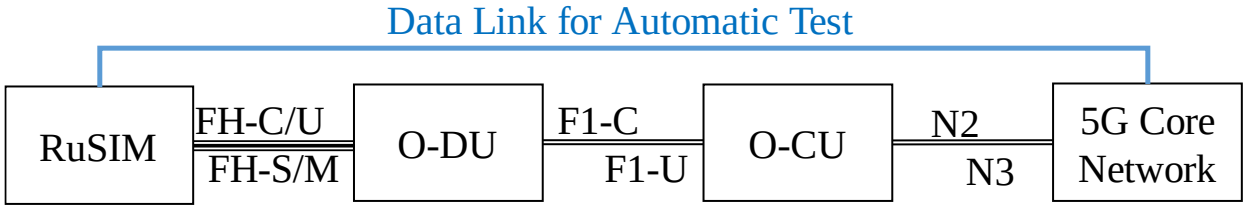
ii. 採用自動測試時，需要透過用戶設備直接分析 RRC 封包與 GTP-U 封包的 PDCP 層內容，且需要透過 5GC 分析 NGAP 封包內容。

(d) 測試佈局：

見圖 18。



(a) 使用 DuSIM 測試



(b) 使用 RuSIM 測試

圖 18 用戶平面資料進行加密測試示意圖

(e) 測試步驟:

(1) 在用戶設備設定支援 NEA1、NEA2、NIA1、NIA2 機密和完整性安全演算法。

(2) 在 O-CU 端設定 NEA1、NIA1 機密和完整性安全演算法為最優先選擇。

(3) 採用工具分析時，開始擷取 F1-C 介面、F1-U 介面及 N2 介面封包。

(4) 確認 O-CU 與 5GC 建立 NGAP 連線，且用戶設備註冊上 5GC 並收送數據資料。

(5) 採用工具分析時，停止擷取 F1-C 介面、F1-U 介面及 N2 介面封包。

(6) 採用工具分析時，透過 F1-C 介面封包，確認用戶設備和 O-CU 完成 RRC 信令安全驗證程序。採用自動測試時，由用戶設備確認。

(7) 採用工具分析時，透過 N2 介面封包，確認 5GC 傳送給 O-CU 的 PDU Session Resource Set Up Request 帶有加密保護需求的安全資訊。採用自動測試時，由 5GC 確認。

(8) 採用工具分析時，透過 F1-C 介面封包，確認 OB-CU 傳送給用戶設備 RRC Reconfiguration 加密保護指示是否符合程序(7)加密保護需求。採用自動測試時，由用戶設備確認。

(9) 將 O-CU 端設定 NEA2、NIA2 機密和完整性安全演算法為最優先選擇後，重複(2)~(8)測試步驟。

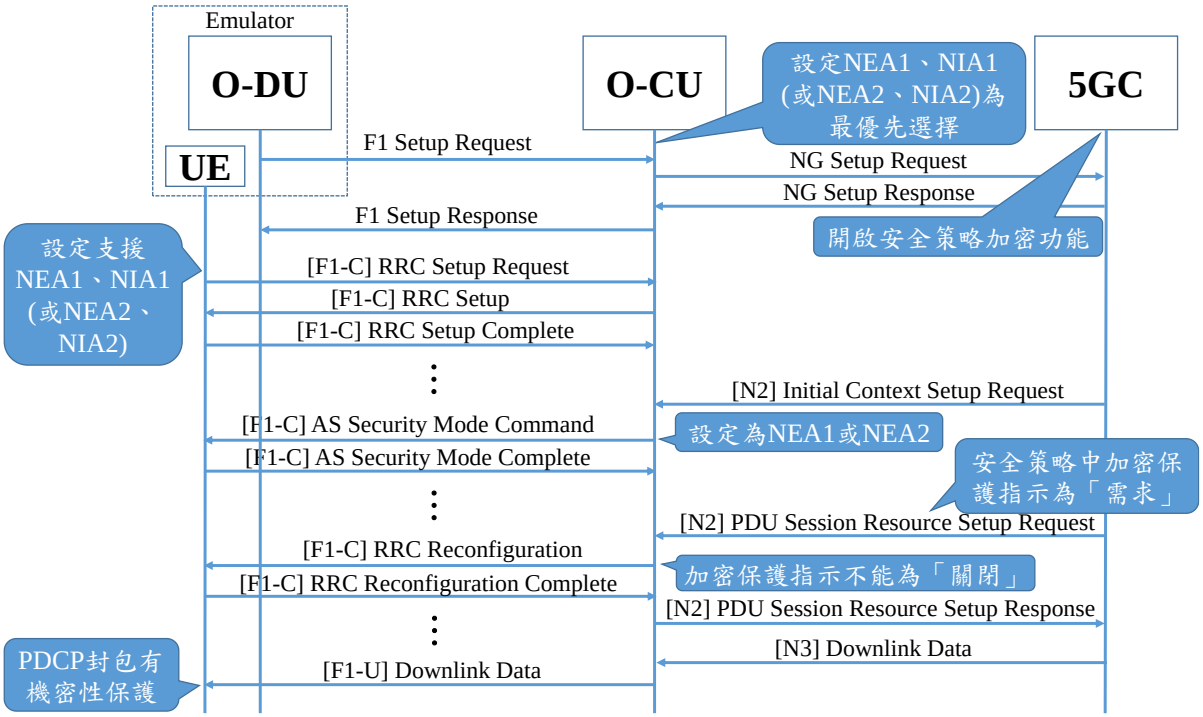


圖 19 用戶平面資料進行加密測試流程圖

(f) 測試結果:

(1) 根據步驟(8)，5GC 傳送的 PDU Session Resource Set Up Request 帶有加密保護需求的安全資訊要為「需求」。

(2) 根據步驟(9)，RRC Reconfiguration 關閉加密保護指示要符合程序(8)加密保護需求要不能為「關閉」。

6.1.2.6 基於連結管理功能(SMF)傳送的安全策略對用戶平面資料進行完整性保護

(a) 測試依據:

依據 3GPP TS 33.501 [11] 之第 5.3.2 小節與 3GPP TR 33.926 [12] 之第 D.2.2.8 小節，並參考 O-RAN TIFG E2E-Test [20] 之第 7.1 小節以及 3GPP TS 33.523 [9] 之第 4.2.2.1.1 小節和 3GPP TS 33.511 [8] 之第 4.2.2.1.11 小節。

(b) 測試目的:

驗證用戶平面資料依據 SMF 的安全策略受到完整性保護。

(c) 測試前提:

(1) 用戶設備及 O-CU 可以設定完整性安全演算法。

(2) SMF 要開啟用戶平面安全策略之用戶平面完整性保護指示。

(3) 用戶設備可以採用 DuSIM 或 RuSIM 之模擬器。

i. 當用戶設備為 DuSIM 時，DuSIM、O-CU 及 5GC 間可以成功建立 5G 連線。

ii. 當用戶設備為 RuSIM 時，RuSIM、O-DU、O-CU 及 5GC 間可以成功建立 5G 連線。

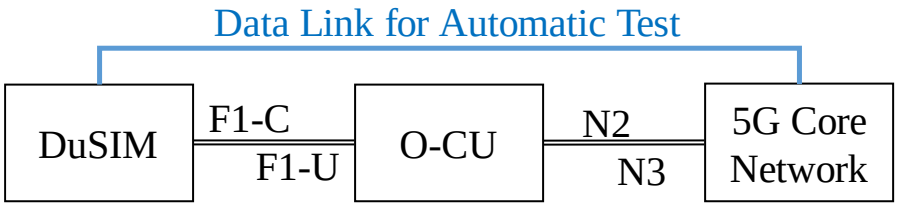
(4) 測試人員可採用分析工具或自動測試。

i. 採用工具分析時，需要擷取 F1-C 介面與 F1-U 介面及 N2 介面封包，並分析 F1-C 介面與 F1-U 介面之 RRC 封包與 GTP-U 封包的 PDCP 層內容，以及分析 N2 介面 NGAP 封包內容。

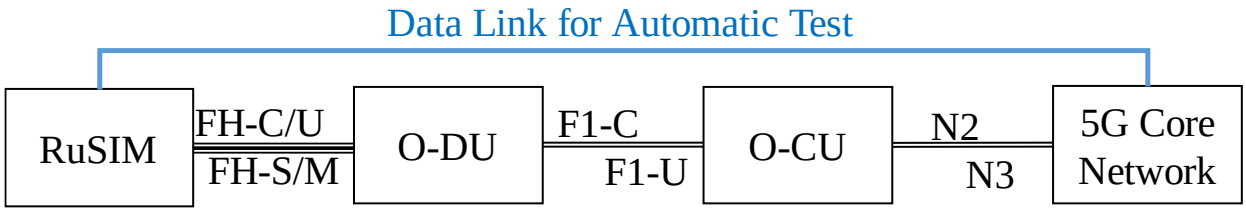
ii. 採用自動測試時，需要透過用戶設備直接分析 RRC 封包與 GTP-U 封包的 PDCP 層內容，但是用戶設備需透過 5GC 分析 NGAP 封包內容。

(d) 測試佈局：

見圖 20。



(a) 使用 DuSIM 測試



(b) 使用 RuSIM 測試

圖 20 用戶平面資料進行完整性保護測試示意圖

(e) 測試步驟:

(1) 在 DuSIM(或 RuSIM)模擬器設定支援 NIA1 和 NIA2 完整性安全演算法。

(2) 在 O-CU 端設定 NIA1 完整性安全演算法為最優先選擇。

(3) 採用工具分析時，開始擷取 F1-C 介面、F1-U 介面及 N2 介面封包。

(4) 確認 O-CU 與 5GC 建立 NGAP 連線，且用戶設備註冊上 5GC 並收送數據資料。

(5) 採用工具分析時，停止擷取 F1-C 介面、F1-U 介面及 N2 介面封包。

(6) 採用工具分析時，透過 F1-C 介面封包，確認用戶設備和 O-CU 完成 RRC 信令安全驗證程序。採用自動測試時，由用戶設備確認。

(7) 採用工具分析時，透過 N2 介面封包，確認 5GC 傳送給 O-CU 的 PDU Session Resource Set Up Request 帶有完整性保護需求的安全資訊。採用自動測試時，由 5GC 確認。

(8) 採用工具分析時，透過 F1-C 介面封包，確認 O-CU 傳送給用戶設備 RRC Reconfiguration 完整性保護指示是否符合程序(8)完整性保護需求。採用自動測試時，由用戶設備確認。

(9) 將 O-CU 端設定 NIA2 完整性安全演算法為最優先選擇後，重複(2)~(8)測試步驟。

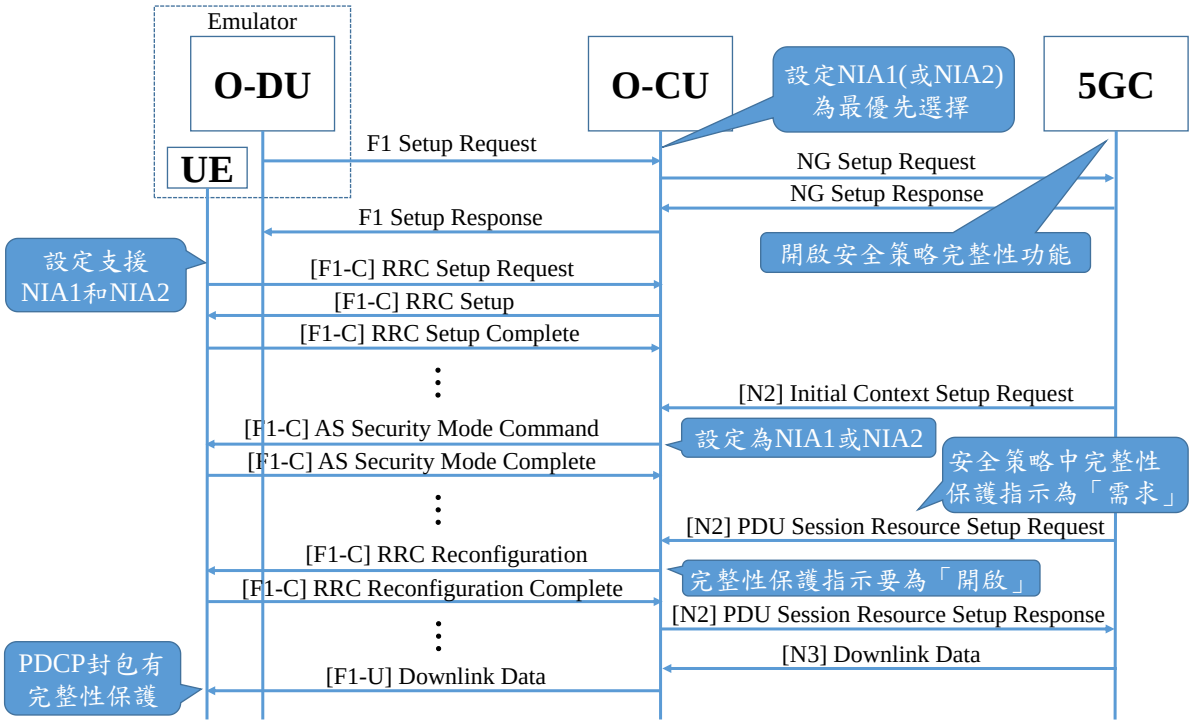


圖 21 用戶平面資料進行完整性保護測試流程圖

(f) 測試結果:

(1) 根據步驟(7)，5GC 傳送的 PDU Session Resource Set Up Request 帶有完整性保護需求的安全資訊要為「需要」。

(2) 根據步驟(8)，RRC Reconfiguration 完整性保護指示要符合程序(7)完整性保護需求要為「開啟」。

6.1.3 O-CU 接取層安全演算法檢測

6.1.3.1 O-CU 接取層加密和完整性演算法優先順序

(a) 測試依據:

依據 3GPP TS 33.501 [11] 之第 5.11.2 小節與 3GPP TR 33.926 [12] 之第 D.2.2.5 小節，並參考 O-RAN TIFG E2E-Test [20] 之第 7.1 小節以及 3GPP TS 33.523 [9] 之第 4.2.2.1.1 小節和 3GPP TS 33.511 [8] 之第 4.2.2.1.12 小節。

(b) 測試目的:

驗證 O-CU 接取層加密和完整性演算法優先順序設定運作正常。

(c) 測試前提:

(1) 用戶設備及 O-CU 可以設定完整性安全演算法。

(2) 用戶設備可以採用 DuSIM 或 RuSIM 之模擬器。

i. 當用戶設備為 DuSIM 時，DuSIM、O-CU 及 5GC 間可以成功建立 5G 連線。

ii. 當用戶設備為 RuSIM 時，RuSIM、O-DU、O-CU 及 5GC 間可以成功建立 5G 連線。

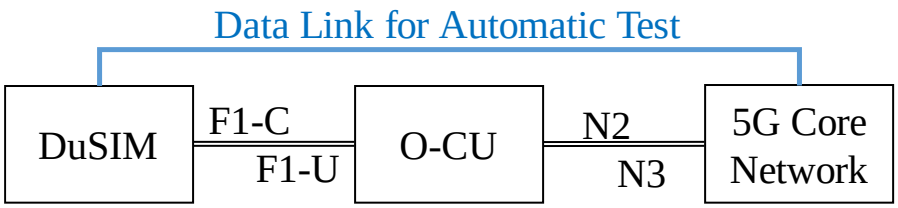
(3) 測試人員可採用分析工具或自動測試。

i. 採用工具分析時，需要擷取 F1-C 介面與 N2 介面封包，並分析 F1-C 介面之 RRC 封包的 PDCP 層內容與 N2 介面 NGAP 封包內容。

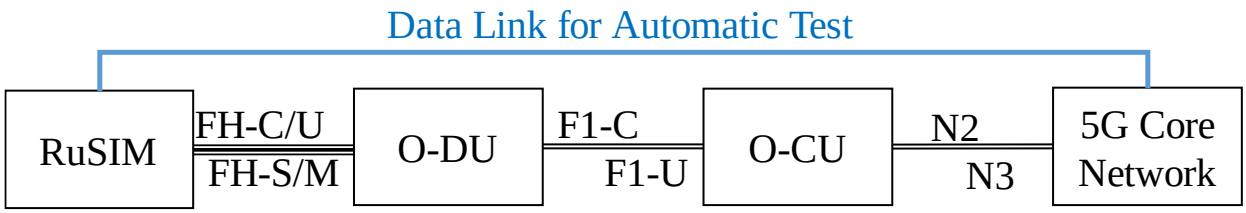
ii. 採用自動測試時，需要透過用戶設備直接分析 RRC 封包的 PDCP 層內容，但是用戶設備需透過 5GC 分析 NGAP 封包內容。

(d) 測試佈局：

見圖 22。



(a) 使用 DuSIM 測試



(b) 使用 RuSIM 測試

圖 22 加密和完整性演算法優先順序測試示意圖

(e) 測試步驟:

(1) 在用戶設備設定支援 NEA1、NEA2、NIA1、NIA2 機密和完整性安全演算法。

(2) 在 O-CU 設定 NEA1、NIA1 機密和完整性安全演算法為最優先選擇。

(3) 採用工具分析時，開始擷取 F1-C 介面和 N2 介面封包。

(4) 確認 O-CU 與 5GC 建立 NGAP 連線，且用戶設備註冊上 5GC。

(5) 採用工具分析時，停止擷取 F1-C 介面和 N2 介面封包。

(6) 採用工具分析時，透過 N2 介面封包，確認 5GC 傳送給 O-CU 的 Initial Context Setup Request 裡面的用戶設備安全能力資訊要為支援 NEA1、NEA2、NIA1、NIA2。採用自動測試時，由 5GC 確認。

(7) 採用工具分析時，透過 F1-C 介面封包，檢查 O-CU 傳送 RRC 信令安全驗證程序需求 AS Security Mode Command 裡面所帶的安全演算法。採用自動測試時，由用戶設備檢查。

(8) 將 O-CU 端設定 NEA2、NIA2 機密和完整性安全演算法為最優先選擇後，重複(2)~(7)測試步驟。

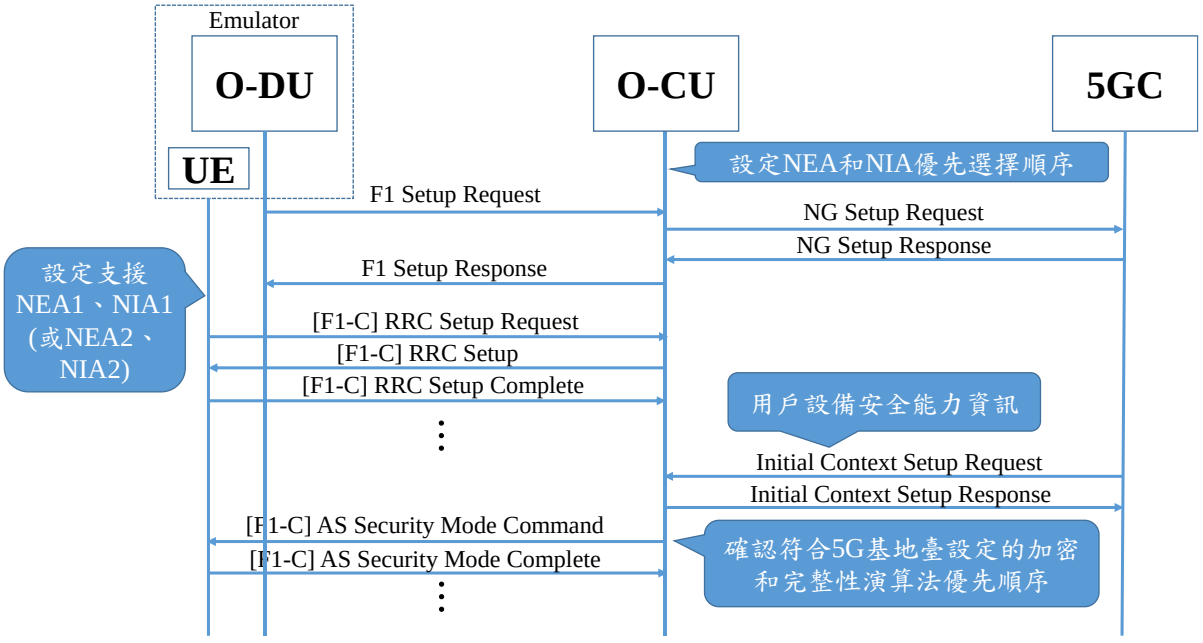


圖 23 加密和完整性演算法優先順序測試流程圖

(f) 測試結果:

(1) 根據步驟(7)，AS Security Mode Command 裡面的安全演算法要符合 O-CU 的安全演算法優先順序設定。

6.1.3.2 O-CU 金鑰更新-重複使用資料無線電承載識別碼

(a) 測試依據:

依據 3GPP TS 33.501 [11] 之第 6.9.4.1 小節與 3GPP TR 33.926 [12] 之第 D.2.2.7 小節，並參考 O-RAN TIFG E2E-Test [20] 之第 7.1 小節以及 3GPP TS 33.523 [9] 之第 4.2.2.1.1 小節和 3GPP TS 33.511 [8] 之第 4.2.2.1.13 小節。

(b) 測試目的:

驗證當達到重複使用資料無線電承載識別碼時，O-CU 金鑰 (K_{gNB}) 更新功能運作正常。

(c) 測試前提:

(1) 用戶設備及 O-CU 可以設定完整性安全演算法。

(2) SMF 如果要開啟用戶平面安全策略，其用戶平面資料加密保護指示不能設定為「停用」。

(3) 測試人員可從用戶設備與 O-CU 擷取安全金鑰 K_{gNB}。

(4) 用戶設備可以採用 DuSIM 或 RuSIM 之模擬器。

i. 當用戶設備為 DuSIM 時，DuSIM、O-CU 及 5GC 間可以成功建立 5G 連線。

ii. 當用戶設備為 RuSIM 時，RuSIM、O-DU、O-CU 及 5GC 間可以成功建立 5G 連線。

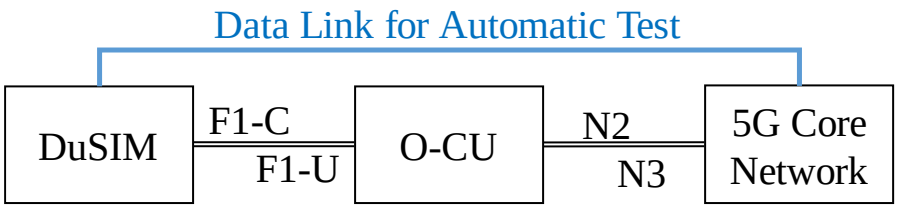
(5) 測試人員可採用分析工具或自動測試。

i. 採用工具分析時，需要擷取 F1-C 介面與 F1-U 介面及 N2 介面封包，並分析 F1-C 介面與 F1-U 介面之 RRC 封包與 GTP-U 封包的 PDCP 層內容，以及分析 N2 介面 NGAP 封包內容。

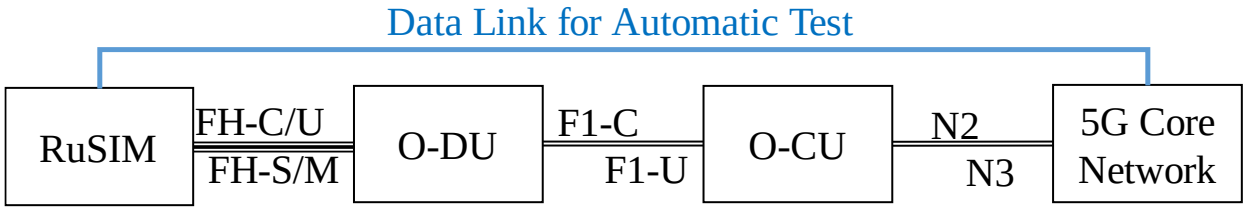
ii. 採用自動測試時，需要透過用戶設備直接分析 RRC 封包與 GTP-U 封包的 PDCP 層內容，但是用戶設備需透過 5GC 分析 NGAP 封包內容。

(d) 測試佈局：

見圖 24。



(a) 使用 DuSIM 測試



(b) 使用 RuSIM 測試

圖 24 O-RAN 基地臺金鑰更新測試示意圖

(e) 測試步驟:

(1) 在用戶設備端設定支援 NIA1 和 NIA2 完整性安全演算法。

(2) O-CU 端設定 NIA1 完整性安全演算法為最優先選擇。

(3) 採用工具分析時，開始擷取 F1-C 介面和 N2 介面封包。

(4) 確認 O-CU 與 5GC 建立 NGAP 連線，且用戶設備註冊上 5GC 並收送數據資料。

(5) 採用工具分析時，停止擷取 F1-C 介面和 N2 介面封包。

(6) 採用工具分析時，透過 N2 介面封包，確認 5GC 傳送給 O-CU 的 PDU Session Resource Set Up Request 帶有完整性保護需求的安全資訊。採用自動測試時，由 5GC 確認。

(7) 採用工具分析時，透過 F1-C 介面封包，確認用戶設備對相同的資料無線電承載進行建立和撤除讓無線電承載識別碼增加直到超過上限發生無線電承載識別碼重覆出現。採用自動測試時，由用戶設備確認。

(8) 確認用戶設備與 O-CU 發生 PDCP 重建進行 K_{gNB} 更新。

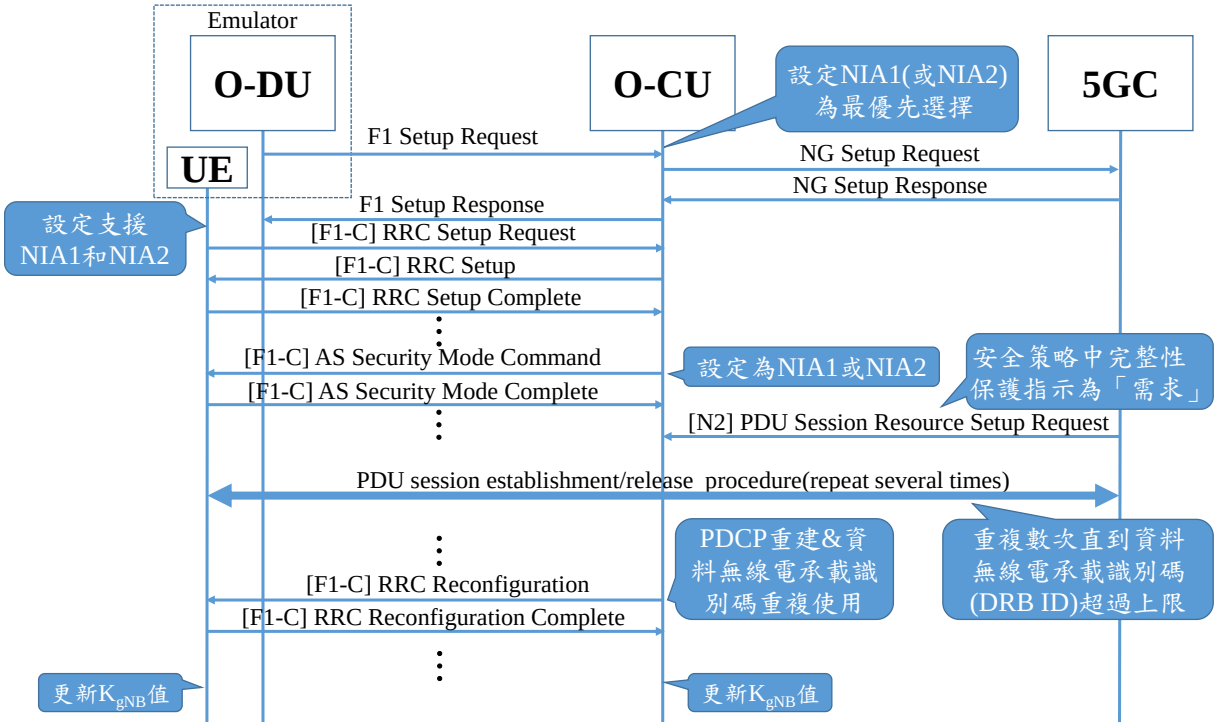


圖 25 O-CU 金鑰更新測試流程圖

(f) 測試結果:

(1) 根據步驟(7)，當無線電承載識別碼重覆使用後，確認用戶設備與 O-CU 間的 PDCP 重建，且用戶設備與 O-CU 間進行 K_{gNB} 更新。

6.1.3.3 O-CU 金鑰金鑰更新-雙連結下封包資料匯聚通訊協定(PDCP)計數環繞

(a) 測試依據：

依據 3GPP TS 33.501 [11] 之第 6.10.2.1、6.10.2.2.1 小節與 3GPP TR 33.926 [12] 之第 D.2.2.7 小節，並參考 O-RAN TIFG E2E-Test [20] 之第 7.1 小節以及 3GPP TS 33.523 [9] 之第 4.2.2.1.1 小節和 3GPP TS 33.511 [8] 之第 4.2.2.1.18 小節。

(b) 測試目的：

驗證次節點之 O-RAN 基地臺當達到封包資料匯聚通訊協定計數環繞時次節點金鑰(K_{SN})更新功能運作正常。

(c) 測試前提：

(1) 本測試案例僅適用於佈建雙連結 (dual connectivity) 的通訊系統。

(2) 用戶設備及 O-CU 可以設定完整性安全演算法。

(3) SMF 如果要開啟用戶平面安全策略，其用戶平面資料加密保護指示不能設定為「停用」。

(4) 測試人員可從用戶設備與 O-CU 擷取安全金鑰 K_{SN}。採用自動測試時，次節點之 O-CU 須為 5gcuSIM 之模擬器。

(5) 用戶設備可以採用 DuSIM 或 RuSIM 之模擬器。

i. 當用戶設備為 DuSIM 時，DuSIM、O-CU 及 5GC 間可以成功建立 5G 連線。

ii. 當用戶設備為 RuSIM 時，RuSIM、O-DU、O-CU 及 5GC 間可以成功建立 5G 連線。

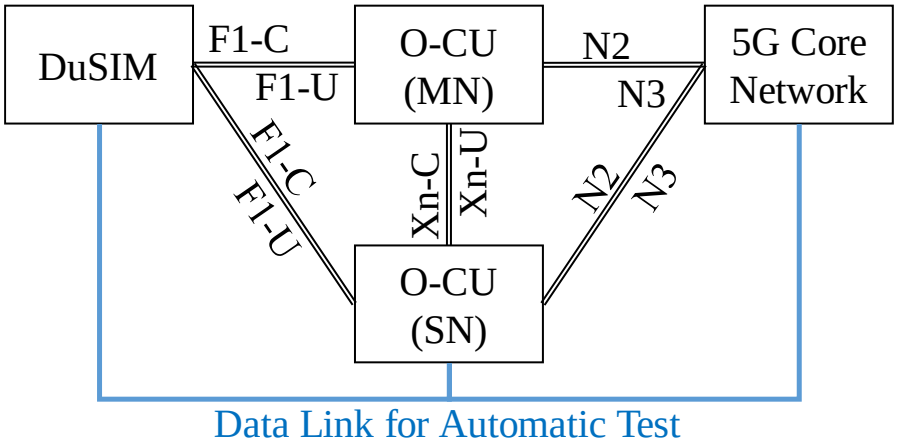
(6) 測試人員可採用分析工具或自動測試。

i. 採用工具分析時，需要擷取 F1-C 介面與 XnAP 介面及 N2 介面封包，並分析 F1-C 介面之 RRC 封包的 PDCP 層內容，與分析 Xn-C 介面 XnAP 封包內容，以及分析 N2 介面 NGAP 封包內容。

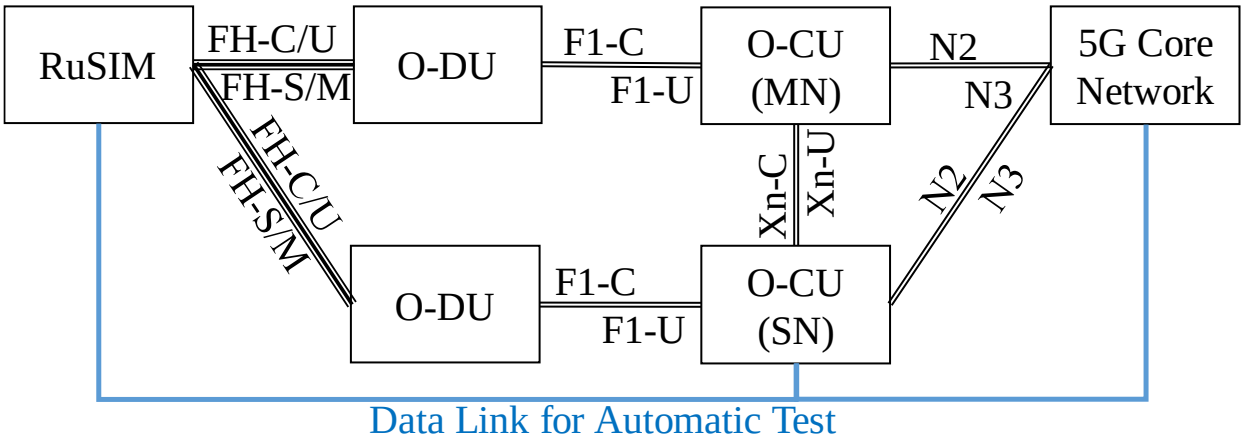
ii. 採用自動測試時，需要透過用戶設備直接分析 RRC 封包的 PDCP 層內容，且需要透過 O-CU 與 5GC 分析 XnAP 封包與 NGAP 封包內容。

(d) 測試佈局：

見圖 26。



(a) 使用 DuSIM 測試



(b) 使用 RuSIM 測試

圖 26 O-RAN 基地臺金鑰更新測試示意圖

(e) 測試步驟：

(1) 在用戶端設定支援 NIA1 和 NIA2 完整性安全演算法。

(2) 在 O-CU 端設定 NIA1 完整性安全演算法為最優先選擇。

(3) 採用工具分析時，開始擷取 Xn 介面和 N2 介面封包。

(4) 確認 O-CU 與 5GC 建立 NGAP 連線，且用戶設備註冊上 5GC 並收送數據資料。

(5) 用戶設備建次節點之 O-CU 連線。

(6) 用戶設備對相同的次節點之 O-CU 傳送 RRC 信令或用戶平面封包直至次節點產生 PDCP 計數環繞 (wrap around)。

(7) 採用工具分析時，停止擷取 F1-C 介面、Xn 介面和 N2 介面封包。

(8) 採用工具分析時，透過 N2 介面封包，確認 5GC 傳送給 O-CU 的 PDU Session Resource Set Up Request 帶有完整性保護需求的安全資訊。採用自動測試時，由 5GC 確認。

(9) 採用工具分析時，透過 F1-C 介面和 Xn 介面封包，觀察 F1-C 介面和 Xn 介面是否啟動次節點金鑰更新流程及 K_{SN} 值狀態。採用自動測試時，由用戶設備需搭配 O-CU 確認。

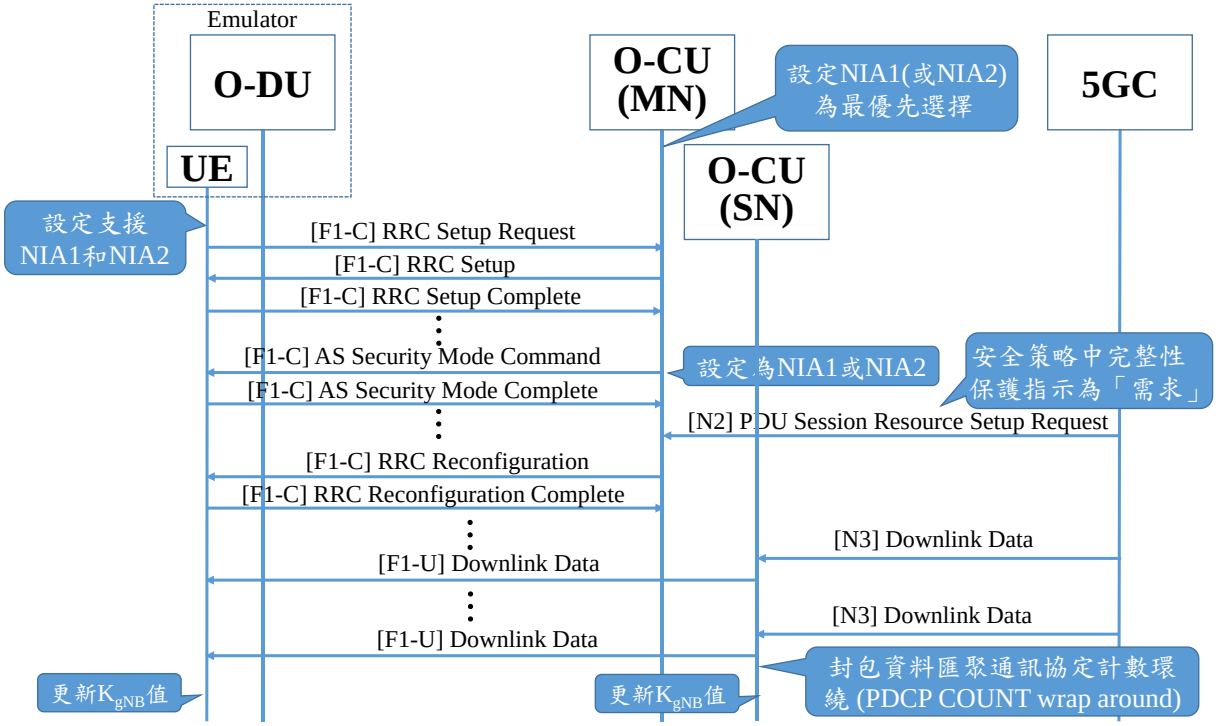


圖 27 次節點之 O-CU 金鑰更新測試流程圖

(f) 測試結果：

(1) 根據步驟(9)，當發生 PDCP 計數環繞後，次節點之 O-CU 會啟動更新金鑰 K_{SN} 避免訊息被洩漏。

6.1.3.4 O-CU 金鑰金鑰更新-雙連結下重複使用資料無線電承載識別碼

(a) 測試依據:

依據 3GPP TS 33.501 [11] 之第 6.10.2.1、6.10.2.2.1 小節與 3GPP [12] 之第 D.2.2.7 小節，並參考 O-RAN TIFG E2E-Test [20] 之第 7.1 小節以及 3GPP TS 33.523 [9] 之第 4.2.2.1.1 小節和 3GPP TS 33.511 [8] 之第 4.2.2.1.18 小節。

(b) 測試目的:

驗證當達到重複使用資料無線電承載識別碼時，次節點金鑰 (K_{SN}) 更新功能運作正常。

(c) 測試前提:

(1) 本測試案例僅適用於佈建雙連結 (dual connectivity) 的通訊系統。

(2) 用戶設備及 O-CU 可以設定完整性安全演算法。

(3) SMF 如果要開啟用戶平面安全策略，其用戶平面資料加密保護指示不能設定為「停用」。

(4) 測試人員可從用戶設備與 O-CU 擷取安全金鑰 K_{SN}。

(5) 用戶設備可以採用 DuSIM 或 RuSIM 之模擬器。

i. 當用戶設備為 DuSIM 時，DuSIM、O-CU 及 5GC 間可以成功建立 5G 連線。

ii. 當用戶設備為 RuSIM 時，RuSIM、O-DU、O-CU 及 5GC 間可以成功建立 5G 連線。

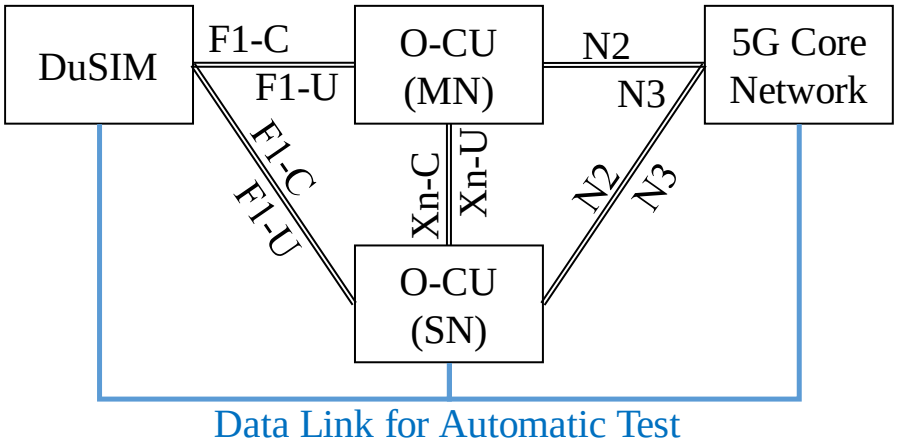
(6) 測試人員可採用分析工具或自動測試。

i. 採用工具分析時，需要擷取 F1-C 介面與 XnAP 介面及 N2 介面封包，並分析 F1-C 介面之 RRC 封包的 PDCP 層內容，與分析 Xn-C 介面 XnAP 封包內容，以及分析 N2 介面 NGAP 封包內容。

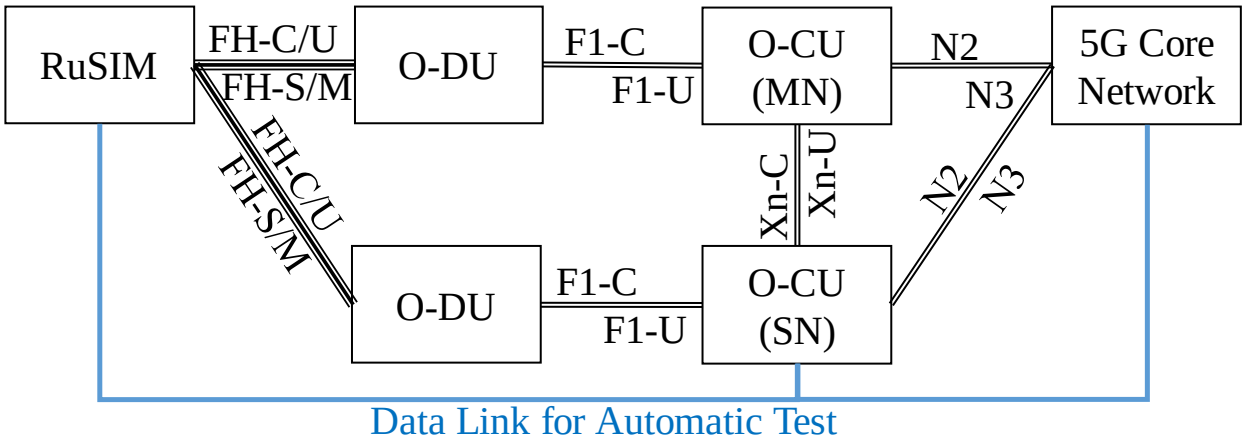
ii. 採用自動測試時，需要透過用戶設備直接分析 RRC 封包的 PDCP 層內容，且需要透過 O-CU 與 5GC 分析 XnAP 封包與 NGAP 封包內容。

(d) 測試佈局：

見圖 28。



(a) 使用 DuSIM 測試



(b) 使用 RuSIM 測試

圖 28 次節點之 O-CU 金鑰更新測試示意圖

(e) 測試步驟:

(1) 在用戶端設定支援 NIA1 和 NIA2 完整性安全演算法。

(2) 在 O-CU 端設定 NIA1 完整性安全演算法為最優先選擇。

(3) 採用工具分析時，開始擷取 F1-C 介面、Xn 介面和 N2 介面封包。

(4) 確認 O-CU 與 5GC 建立 NGAP 連線，且用戶設備註冊上 5GC 並收送數據資料。

(5) 用戶設備建次節點之 O-CU 連線。

(6) 用戶設備在次節點對相同的資料無線電承載進行建立和撤除讓無線電承載識別碼增加直到超過上限發生無線電承載識別碼重覆出現。

(7) 採用工具分析時，停止擷取 F1-C 介面、Xn 介面和 N2 介面封包。

(8) 採用工具分析時，透過 N2 介面封包，確認 5GC 傳送給 O-CU 的 PDU Session Resource Set Up Request 帶有完整性保護需求的安全資訊。採用自動測試時，由 5GC 確認。

(9) 採用工具分析時，透過 F1-C 介面和 Xn 介面封包，觀察 F1-C 介面和 Xn 介面是否啟動次節點金鑰更新流程及 K_{SN} 值狀態。採用自動測試時，由用戶設備需搭配 O-CU 確認。

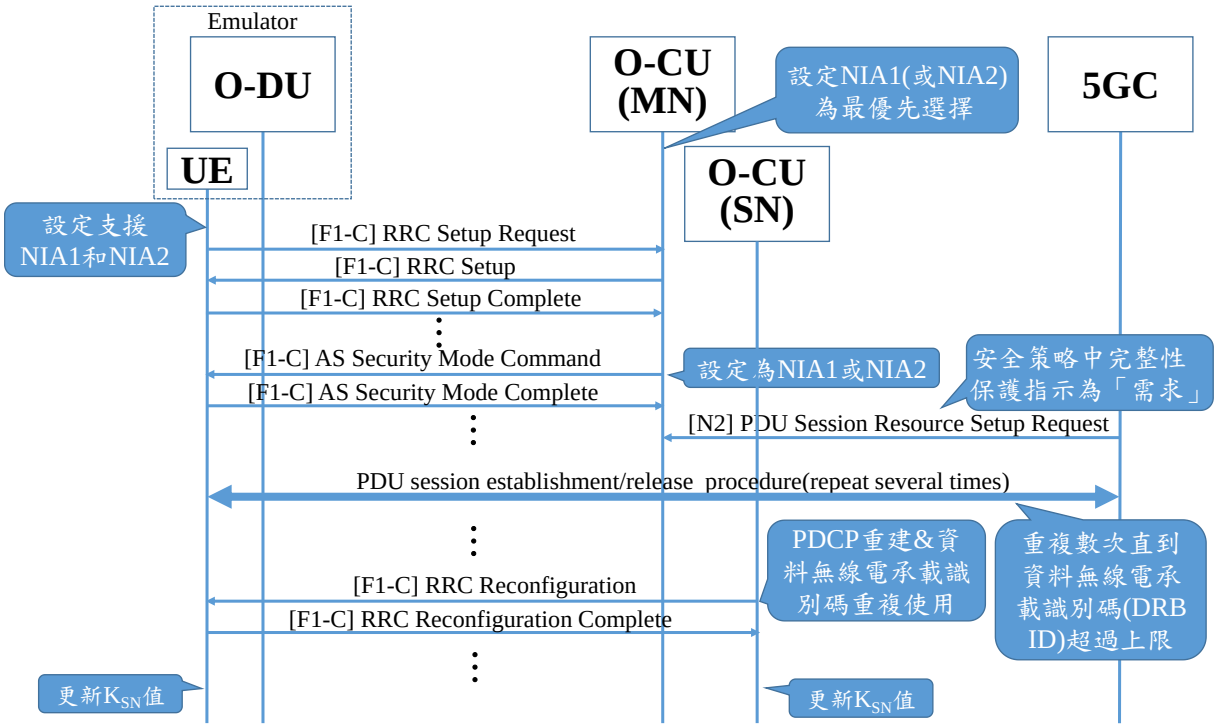


圖 29 O-RAN 基地臺金鑰更新測試流程圖

(f) 測試結果:

(1) 根據步驟(9)，當發生重複使用資料無線電承載識別碼後，次節點之 O-CU 會啟動次節點金鑰更新使 K_{SN} 進行更新避免訊息被洩漏。

6.1.4 O-CU 變更安全演算法保護

6.1.4.1 防範 Xn 介面交遞中的降階攻擊

(a) 測試依據:

依據 3GPP TS 33.501 [11] 之第 6.7.3.1 小節與 3GPP TR 33.926 [12] 之第 D.2.2.6 小節，並參考 O-RAN TIFG E2E-Test [20] 之第 7.1 小節以及 3GPP TS 33.523 [9] 之第 4.2.2.1.1 小節和 3GPP TS 33.511 [8] 之第 4.2.2.1.14 小節。

(b) 測試目的:

驗證當發生 Xn 交遞時預防降階攻擊的檢查機制。

(c) 測試前提:

(1) 用戶設備、來源 O-CU 及目的 O-CU 可以設定完整性安全演算法。

(2) 來源 O-CU 及目的 O-CU 間可以支援 Xn 介面換手(handover)。採用自動測試時，來源 O-CU 須為 5gcuSIM 之模擬器。

(3) 用戶設備可以採用 DuSIM 或 RuSIM 之模擬器。

i. 當用戶設備為 DuSIM 時，DuSIM、來源 O-CU 及 5GC 間可以成功建立 5G 連線，且 DuSIM、目的 O-CU 及 5GC 間可以成功建立 5G 連線。

ii. 當用戶設備為 RuSIM 時，RuSIM、來源 O-DU、來源 O-CU 及 5GC 間可以成功建立 5G 連線，RuSIM、目的 O-DU、目的 O-CU 及 5GC 間可以成功建立 5G 連線。

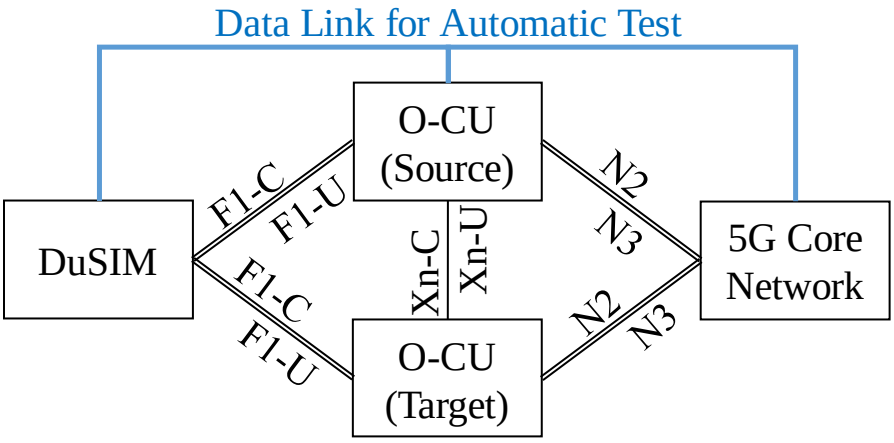
(4) 測試人員可採用分析工具或自動測試。

i. 採用工具分析時，需要擷取 XnAP 介面與 N2 介面封包，並分析 Xn-C 介面 XnAP 封包內容，與分析 N2 介面 NGAP 封包內容。

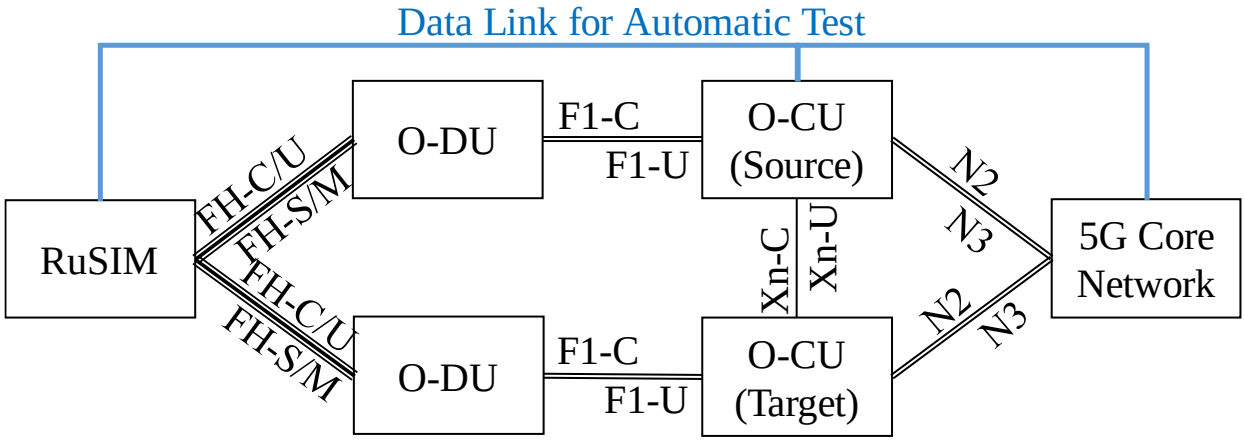
ii. 採用自動測試時，用戶設備需透過 O-CU 與 5GC 分析 XnAP 封包與 NGAP 封包內容。

(d) 測試佈局：

見圖 30。



(a) 使用 DuSIM 與 5gcuSIM 測試



(b) 使用 RuSIM 測試

圖 30 防範 Xn 交遞中的降階攻擊測試示意圖

(e) 測試步驟:

(1) 在用戶設備設定支援 NEA1、NEA2、NIA1、NIA2 機密性和完整性安全演算法。

(2) 在來源 O-CU 及目的 O-CU 端設定 NEA1、NIA1 機密性和完整性安全演算法為最優先選擇。

(3) 採用工具分析時，開始擷取 F1-C 介面、N2 介面和 Xn-C 介面封包。

(4) 確認來源 O-CU 及目的 O-CU 與 5GC 建立 NGAP 連線，且用戶設備透過來源 O-CU 註冊上 5GC。

(5) 用戶設備進行換手(handover)，確認用戶設備與來源 O-CU 及目的 O-CU 和 5GC 完成 Xn 介面換手程序。

(6) 採用工具分析時，停止擷取 F1-C 介面、N2 介面和 Xn-C 介面封包。

(7) 採用工具分析時，透過 Xn-C 介面封包，檢查應用協定路徑切換信令內容並確認完成路徑切換信令。採用自動測試時，由 O-CU 確認。

(8) 採用工具分析時，透過 N2 介面封包，檢查應用協定路徑切換信令內容並確認完成路徑切換信令。採用自動測試時，由 5GC 確認。

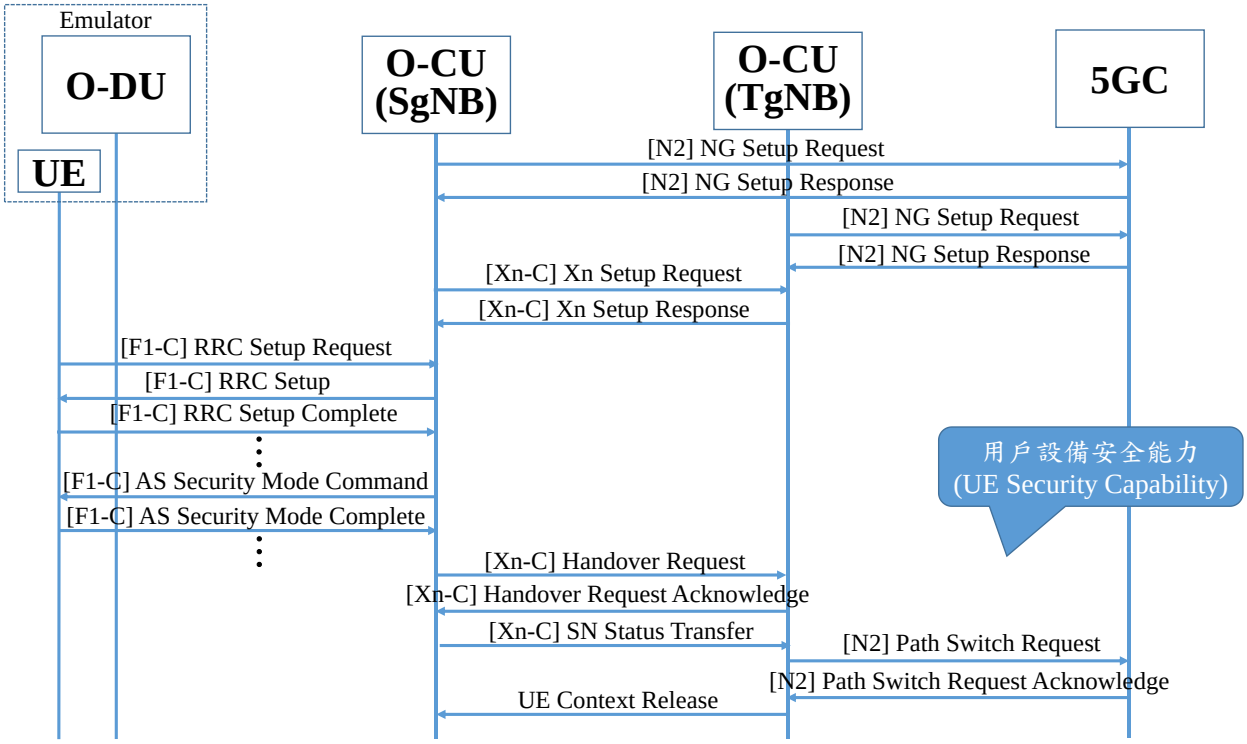


圖 31 防範 Xn 交遞中的降階攻擊測試流程圖

(f) 測試結果:

(1) 根據步驟(7)，確認路徑切換信令裡面的用戶設備安全能力 (UE 5G Security Capability) 要和用戶設備支援的安全能力相同。

6.1.4.2 在 Xn 介面交遞中接取層安全演算法選擇

(a) 測試依據:

依據 3GPP TS 33.501 [11] 之第 6.7.3.1、6.7.3.2 小節與 3GPP [12] 之第 D.2.2.5 小節，並參考 O-RAN TIFG E2E-Test [20] 之第 7.1 小節以及 3GPP TS 33.523 [9] 之第 4.2.2.1.1 小節和 3GPP TS 33.511 [8] 之第 4.2.2.1.15 小節。

(b) 測試目的:

驗證當發生 Xn 交遞時接取層安全演算法選擇機制。

(c) 測試前提:

(1) 用戶設備、來源 O-CU 及目的 O-CU 可以設定完整性安全演算法。

(2) 來源 O-CU 及目的 O-CU 間可以支援 Xn 介面換手(handover)。

(3) 用戶設備可以採用 DuSIM 或 RuSIM 之模擬器。

i. 當用戶設備為 DuSIM 時，DuSIM、來源 O-CU 及 5GC 間可以成功建立 5G 連線，且 DuSIM、目的 O-CU 及 5GC 間可以成功建立 5G 連線。

ii. 當用戶設備為 RuSIM 時，RuSIM、來源 O-DU、來源 O-CU 及 5GC 間可以成功建立 5G 連線，RuSIM、目的 O-DU、目的 O-CU 及 5GC 間可以成功建立 5G 連線。

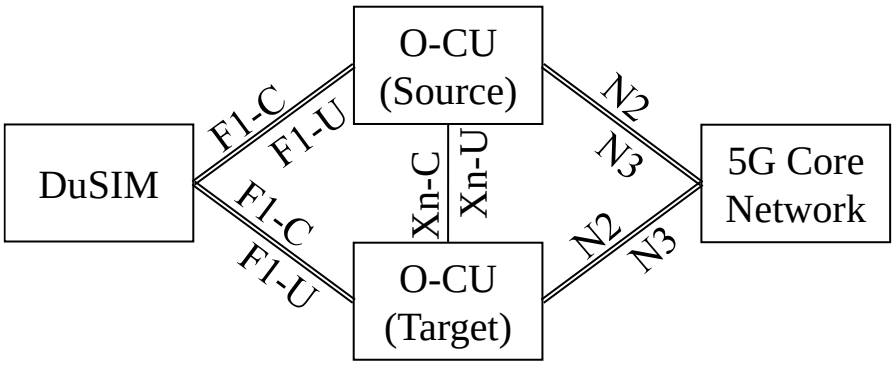
(4) 測試人員可採用分析工具或自動測試。

i. 採用工具分析時，需要擷取 F1-C 介面封包，並分析 F1-C 介面之 RRC 封包的 PDCP 層內容。

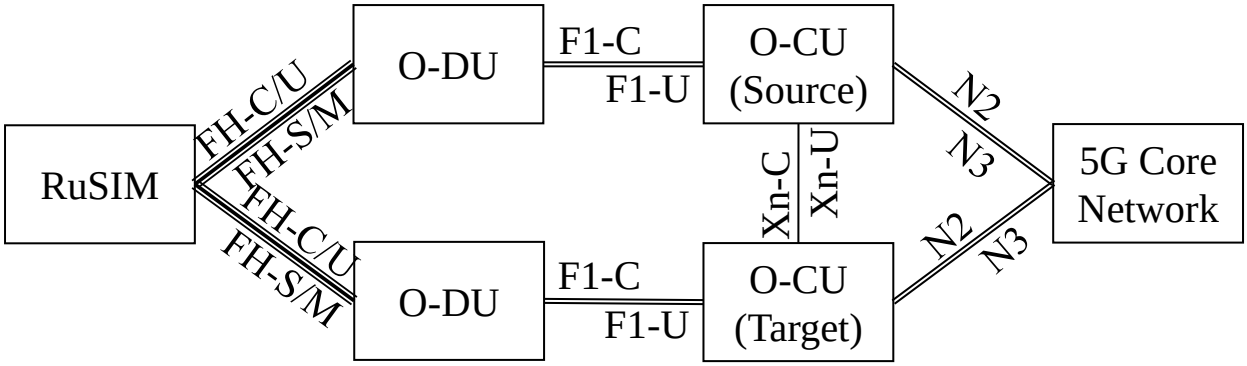
ii. 採用自動測試時，需要透過用戶設備分析 RRC 封包的 PDCP 層內容。

(d) 測試佈局：

見圖 32。



(a) 使用 DuSIM 測試



(b) 使用 RuSIM 測試

圖 32 在 Xn 交遞中接取層安全演算法選擇測試示意圖

(e) 測試步驟:

(1) 在用戶設備設定支援 NEA1、NEA2、NIA1、NIA2 機密性和完整性安全演算法。

(2) 在來源 O-CU 及目的 O-CU 端設定 NEA1、NIA1 機密性和完整性安全演算法為最優先選擇。

(3) 採用工具分析時，開始擷取 F1-C 介面封包。

(4) 確認來源 O-CU 及目的 O-CU 與 5GC 建立 NGAP 連線，且用戶設備透過來源 O-CU 註冊上 5GC。

(5) 用戶設備進行換手(handover)，確認用戶設備與來源 O-CU 及目的 O-CU 和 5GC 完成 Xn 介面換手程序。

(6) 採用工具分析時，停止擷取 F1-C 介面封包。

(7) 採用工具分析時，透過 F1-C 介面，檢查 RRC Reconfiguration 中的目的 O-RAN 基地臺的加密和完整性安全演算法。採用自動測試時，由用戶設備檢查。

(8) 採用工具分析時，透過 F1-C 介面，確認用戶設備回復 RRC Reconfiguration Complete。採用自動測試時，由用戶設備確認。

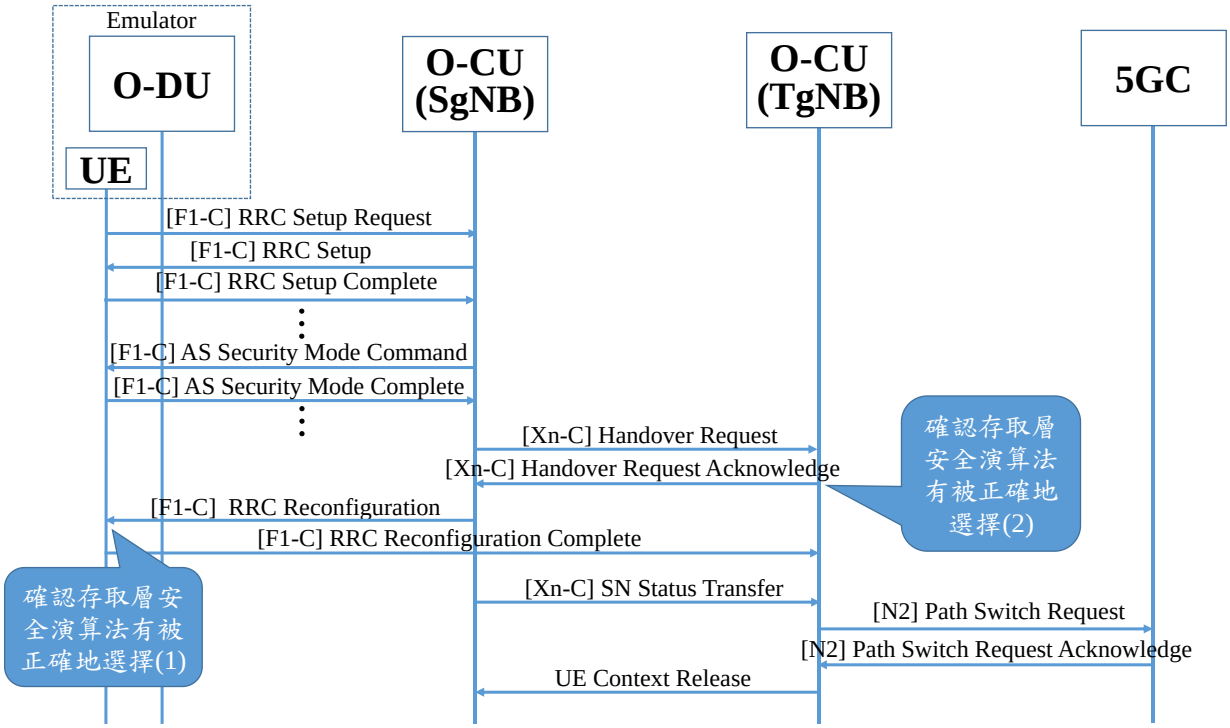


圖 33 在 Xn 交遞中接取層安全演算法選擇測試流程圖

(f) 測試結果:

(1) 根據步驟(7)，RRC Reconfiguration 中的目的 O-CU 的加密和完整性安全演算法要符合目的 O-CU 的安全演算法優先順序設定。

(2) 並且用戶設備會回復 RRC Connection Reconfiguration Complete。

6.1.5 O-CU 安全通道檢測

6.1.5.1 控制平面資料在 N2 介面的機密性保護

依據 TAICS TS-0035 5G 基地臺資安測試規範的 6.1.5.1 節定義之測試流程。

6.1.5.2 用戶平面資料在 N3 介面的機密性保護

依據 TAICS TS-0035 5G 基地臺資安測試規範的 6.1.5.2 節定義之測試流程。

6.1.5.3 控制平面資料在 Xn-C 介面的機密性保護

依據 TAICS TS-0035 5G 基地臺資安測試規範的 6.1.5.3 節定義之測試流程。

6.1.5.4 控制平面資料在 F1-C 介面的機密性保護

(a) 測試依據：

依據 3GPP TS 33.501 [11] 之第 5.3.9 小節與 O-RAN Security Test Specification[15]之第 6.5 小節，並參考 3GPP TS 33.210 [14] 之第 5.3.3 和 5.3.4 小節以及 3GPP TS 33.523 [9]之第 4.2.2.1.2 小節。

(b) 測試目的：

驗證待測物 O-CU 的 F1-C 介面控制平面資料符合網際網路安全協定 (IPsec) 加密和認證達到機密性保護。

(c) 測試前提：

(1) 用戶設備及待測物 O-CU 間可以進行接取層安全演算法設定。

(2) 與待測物的安全閘道器可以成功建立 IPsec 連線。

(3) 用戶設備可以採用 DuSIM 或 RuSIM 之模擬器。

i. 當用戶設備為 DuSIM 時，DuSIM 與待測物 O-CU 間可以成功透過 IPsec 建立 F1AP 連線，且 DuSIM、待測物 O-CU 及 5GC 間可以成功建立 5G 連線。

ii. 當用戶設備為 RuSIM 時，O-DU 與待測物 O-CU 間可以成功透過 IPsec 建立 F1AP 連線，且 RuSIM、O-DU、待測物 O-CU 及 5GC 間可以成功建立 5G 連線。

(4) 待測物的安全閘道器(Security Gateway, SeGW)都可以支援 IKEv2，並可進行 IPsec 安全演算法設定。

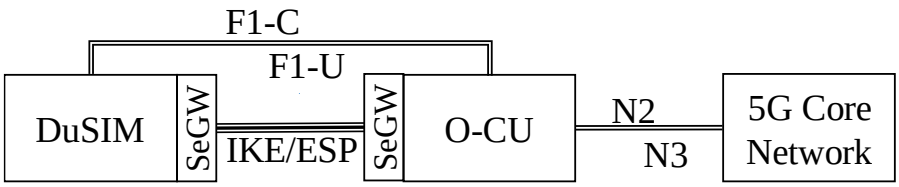
(5) 測試人員可採用分析工具或自動測試。

i. 採用工具分析時，需要擷取並解密 IPsec 介面封包，並分析 ISAKMP 與封裝安全承載內容。

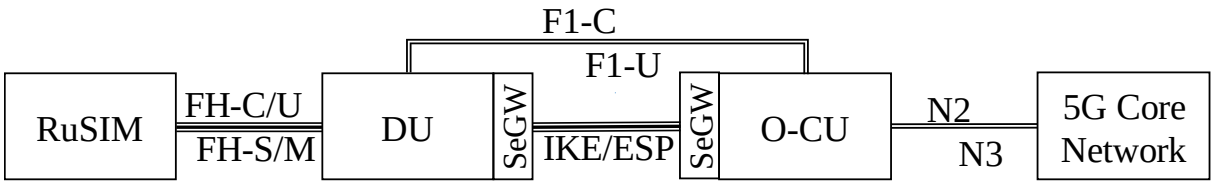
ii. 採用自動測試時，需要透過 DuSIM 的 SeGW 直接解密 IPsec 介面封包，並分析 ISAKMP 與封裝安全承載內容。

(d) 測試佈局：

見圖 34。



(a) 使用 DuSIM 測試



(b) 使用 RuSIM 測試

圖 34 控制平面資料在 F1-C 介面機密性保護測試示意圖

(e) 測試步驟：

(1) 在用戶設備設定支援 NEA1、NEA2、NIA1、NIA2 機密和完整性安全演算法。

(2) 在待測物 O-CU 端設定 NEA1、NIA1 機密和完整性安全演算法為最優先選擇。

(3) 採用工具分析時，開始擷取 IPsec 介面封包。

(4) 與待測物的安全閘道器建立 IPsec 連線。

(5) 採用工具分析時，用戶設備可以採用 DuSIM 或 RuSIM 之模擬器。採用自動測試時，用戶設備只能使用 DuSIM。

i. 當用戶設備為 DuSIM 時，確認 DuSIM 與待測物 O-CU 間成功透過 IPsec 建立 F1AP 連線。

ii. 當用戶設備為 RuSIM 時，確認 RuSIM 與待測物 O-DU 建立 Open FH 連線，且 O-DU 與待測物 O-CU 成功透過 IPsec 建立 F1AP 連線。

(6) 確認待測物 O-CU 與 5GC 建立 NGAP 連線，且用戶設備註冊上 5GC。

(7) 採用工具分析時，停止擷取 IPsec 介面封包。

(8) 採用工具分析時，透過 IPsec 介面封包，確認完成 IKE-SA-INIT 和 IKE-AUTH 程序並解密檢查其中之加密演算法。採用自動測試時，透過 DuSIM 端確認。

(9) 採用工具分析時，透過 IPsec 介面封包，確認使用封裝安全承載量進行資料傳輸並解密其封包。採用自動測試時，透過 DuSIM 端確認。

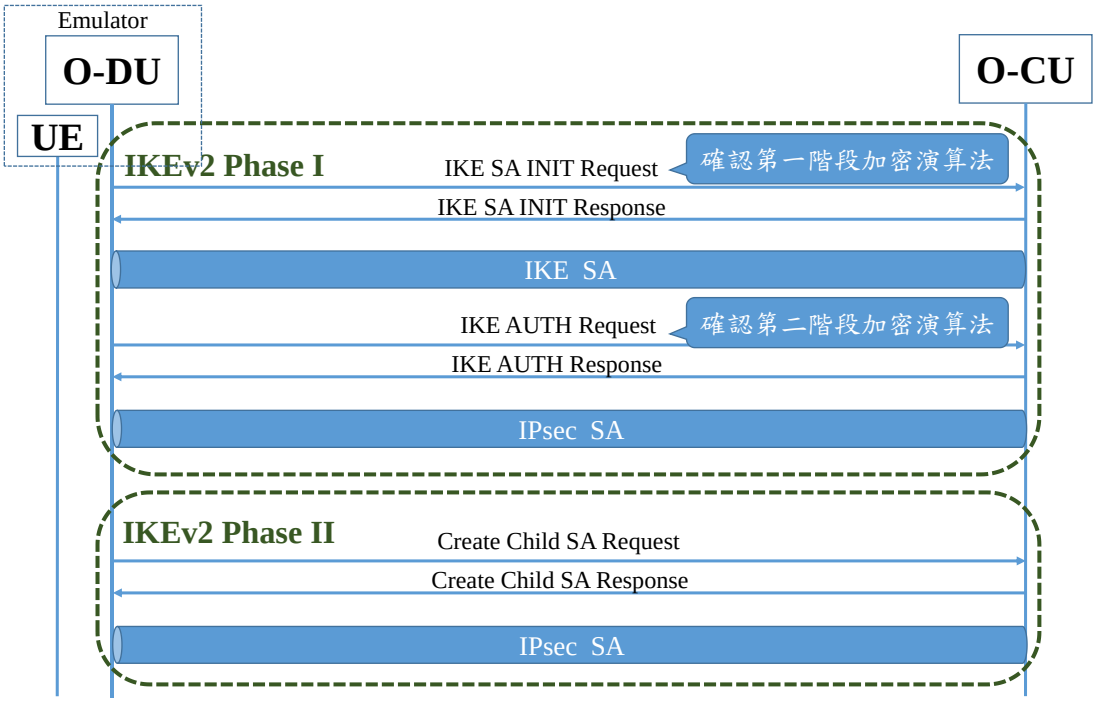


圖 35 控制平面資料在 F1-C 介面機密性保護測試流程圖

(f) 測試結果：

(1) 根據步驟(8)，IKE-SA-INIT 請求信令中含有 IKEv2 的第一階段加密演算法應符合以下標準。根據 3GPP REL 15 與 REL 16，其演算法支援等級分為必須支援的 Shall 和建議支援的 Should。

3GPP REL 15

i AES-CBC with 128-bit key length - Shall

ii AES-GCM with a 16 octet ICV with 128-bit key length - Shall

iii AES-GCM with a 16 octet ICV with 256-bit key length – Should

3GPP REL 16

i AES-GCM with a 16 octet ICV with 128-bit key length - Shall

ii AES-GCM with a 16 octet ICV with 256-bit key length – Should

(2) 根據步驟(8)，IKE-AUTH 是由 IKEv2 的第一階段加密演算法進行機密性保護。解密後的 IKE-AUTH 請求信令中含有 IKEv2 的第二階加密演算法應符合以下標準。其演算法支援等級分為必須支援的 Shall，標記+代表演算法強度更強。

i AES-CBC with 128-bit key length - Shall

ii AES-CBC with 256-bit key length - Shall+

iii AES-GCM with a 16 octet ICV with 128-bit key length - Shall

iv AES-GCM with a 16 octet ICV with 256-bit key length - Shall+

(3) 根據步驟(9)，封裝安全承載量資料封包是由 IKEv2 的第二階加密演算法進行機密性保護，將其解密後得到 F1AP 資料封包。

6.1.5.5 用戶平面資料在 F1-U 介面的機密性保護

(a) 測試依據：

依據 3GPP TS 33.501 [11] 之第 5.3.9 小節與 O-RAN Security Test Specification[15]之第 6.5 小節，並參考 3GPP TS 33.210 [14] 之第 5.3.3 和 5.3.4 小節以及 3GPP TS 33.523 [9]之 4.2.2.1.4 小節。

(b) 測試目的：

驗證待測物 O-CU 的 F1-U 介面用戶平面資料符合網際網路安全協定 (IPsec) 加密和認證達到機密性保護。

(c) 測試前提：

(1) 用戶設備及待測物 O-CU 間可以進行接取層安全演算法設定。

(2) 與待測物的安全閘道器可以成功建立 IPsec 連線。

(3) 用戶設備可以採用 DuSIM 或 RuSIM 之模擬器。

i. 當用戶設備為 DuSIM 時，DuSIM 與待測物 O-CU 間可以成功透過 IPsec 建立 F1AP 連線，且 DuSIM、待測物 O-CU 及 5GC 間可以成功建立 5G 連線。

ii. 當用戶設備為 RuSIM 時，O-DU 與待測物 O-CU 間可以成功透過 IPsec 建立 F1AP 連線，且 RuSIM、O-DU、待測物 O-CU 及 5GC 間可以成功建立 5G 連線。

(4) 待測物的安全閘道器(Security Gateway, SeGW)可以支援 IKEv2，並可進行 IPsec 安全演算法設定。

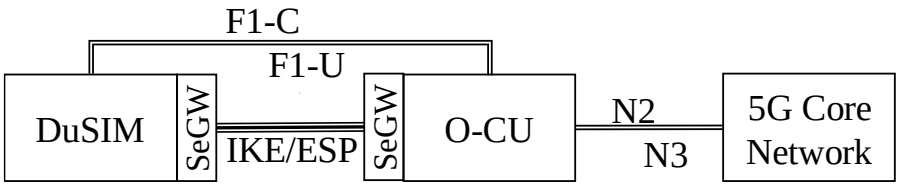
(5) 測試人員可採用分析工具或自動測試。

i. 採用工具分析時，需要擷取並解密 IPsec 介面封包，並分析 ISAKMP 與封裝安全承載內容。

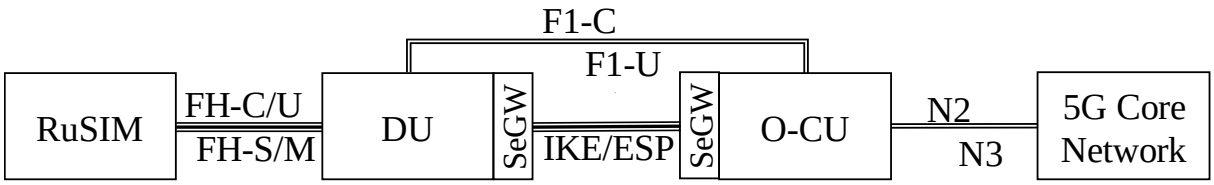
ii. 採用自動測試時，需要透過 DuSIM 的 SeGW 直接解密 IPsec 介面封包，並分析 ISAKMP 與封裝安全承載內容。

(d) 測試佈局：

見圖 36。



(a) 使用 DuSIM 測試



(b) 使用 RuSIM 測試

圖 36 用戶平面資料在 F1-U 介面機密性保護測試示意圖

(e) 測試步驟：

(1) 在用戶設備設定支援 NEA1、NEA2、NIA1、NIA2 機密和完整性安全演算法。

(2) 在待測物 O-CU 端設定 NEA1、NIA1 機密和完整性安全演算法為最優先選擇。

(3) 採用工具分析時，開始擷取 IPsec 介面封包。

(4) 待測物的安全閘道器建立 IPsec 連線。

(5) 採用工具分析時，用戶設備可以採用 DuSIM 或 RuSIM 之模擬器。採用自動測試時，用戶設備只能使用 DuSIM。

i. 當用戶設備為 DuSIM 時，確認 DuSIM 與待測物 O-CU 間成功透過 IPsec 建立 F1AP 連線。

ii. 當用戶設備為 RuSIM 時，確認 RuSIM 與 O-DU 建立 Open FH 連線，且 O-DU 與待測物 O-CU 成功透過 IPsec 建立 F1AP 連線。

(6) 確認待測物 O-CU 與 5GC 建立 NGAP 連線，且用戶設備註冊上 5GC 並收送數據資料。

(7) 採用工具分析時，停止擷取 IPsec 介面封包。

(8) 採用工具分析時，透過 IPsec 介面封包，確認完成 IKE-SA-INIT 和 IKE-AUTH 程序並解密檢查其中之加密演算法。採用自動測試時，透過 DuSIM 端確認。

(9) 採用工具分析時，透過 IPsec 介面封包，確認使用封裝安全承載量進行資料傳輸並解密其封包。採用自動測試時，透過 DuSIM 端確認。

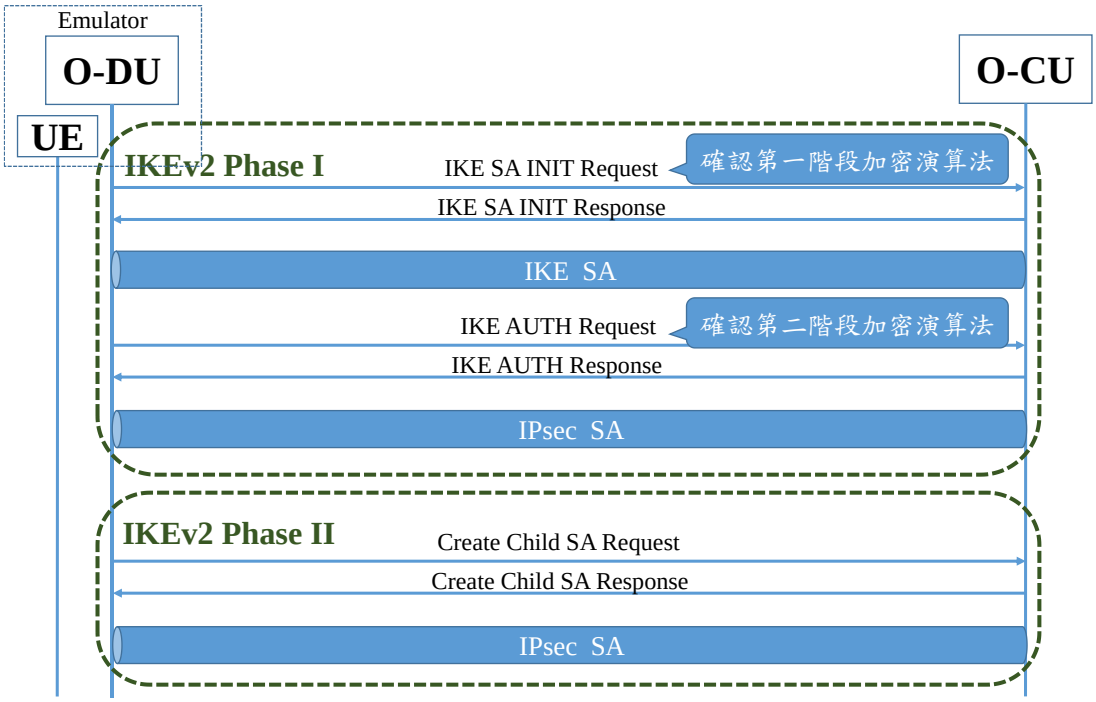


圖 37 用戶平面資料在 F1-U 介面機密性保護測試流程圖

(f) 測試結果：

(1) 根據步驟(8)，IKE-SA-INIT 請求信令中含有 IKEv2 的第一階段加密演算法應符合以下標準。根據 3GPP REL 15 與 REL 16，其演算法支援等級分為必須支援的 Shall 和建議支援的 Should。

3GPP REL 15

i AES-CBC with 128-bit key length - Shall

ii AES-GCM with a 16 octet ICV with 128-bit key length - Shall

iii AES-GCM with a 16 octet ICV with 256-bit key length – Should

3GPP REL 16

i AES-GCM with a 16 octet ICV with 128-bit key length - Shall

ii AES-GCM with a 16 octet ICV with 256-bit key length – Should

(2) 根據步驟(8)，IKE-AUTH 是由 IKEv2 的第一階段加密演算法進行機密性保護。解密後的 IKE-AUTH 請求信令中含有 IKEv2 的第二階加密演算法應符合以下標準。其演算法支援等級分為必須支援的 Shall，標記+代表演算法強度更強。

i AES-CBC with 128-bit key length - Shall

ii AES-GCM with a 16 octet ICV with 128-bit key length - Shall

iv AES-GCM with a 16 octet ICV with 256-bit key length - Shall+

(3) 根據步驟(9)，封裝安全承載量資料封包是由 IKEv2 的第二階加密演算法進行機密性保護，將其解密後得到 F1-U 介面之用戶平面資料封包。

6.1.5.6 控制平面資料在 E2 介面的機密性保護

(a) 測試依據：

依據 O-RAN Security Test Specification [15]之 6.5 和 13.2 小節，並參考 O-RAN Security Protocols Specification [19]之第 2.2 小節與 3GPP TS 33.210 [14] 之第 5.3.3 和 5.3.4 小節。

(b) 測試目的：

驗證待測物 O-CU 的 E2 介面控制平面資料符合網際網路安全協定 (IPsec) 加密和認證達到機密性保護。

(c) 測試前提：

(1) 用戶設備及待測物 O-CU 間可以進行接取層安全演算法設定。

(2) 與待測物的安全閘道器間可以成功建立 IPsec 連線。

(3) 待測物 O-CU 與 Near-RT RIC 間可以成功透過 IPsec 建立 E2AP 連線。

(4) 用戶設備採用 DuSIM 與 Near-RT RicSIM 間可以成功透過 IPsec 建立 E2AP 連線，且 DuSIM、待測物 O-CU 及 5GC 間可以成功建立 5G 連線。採用自動測試時，Near-RT RIC 需為 RicSIM。

(5) 待測物的安全閘道器(Security GatewaySeGW)可以支援 IKEv2，並可進行 IPsec 安全演算法設定。

(6) 測試人員可採用分析工具或自動測試。

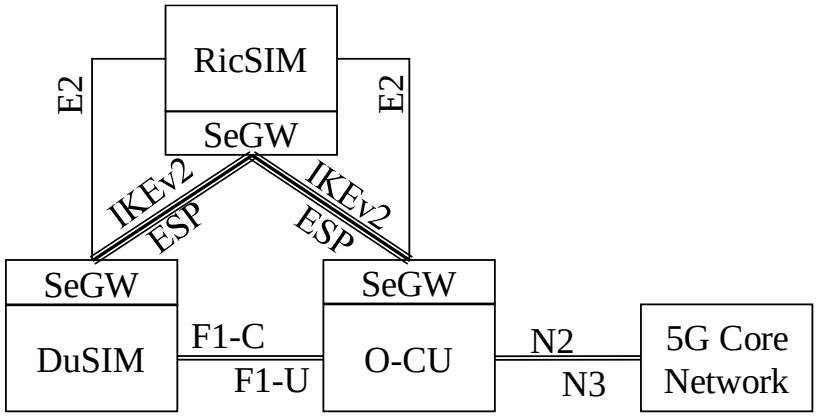
i 採用工具分析時，需要擷取並解密 IPsec 介面封包，並分析 ISAKMP 與封裝安全承載內容。

ii 採用自動測試時，需要透過 RicSIM 的 SeGW 直接解密 IPsec 介面封包，並分析 ISAKMP 與封裝安全承載內容。

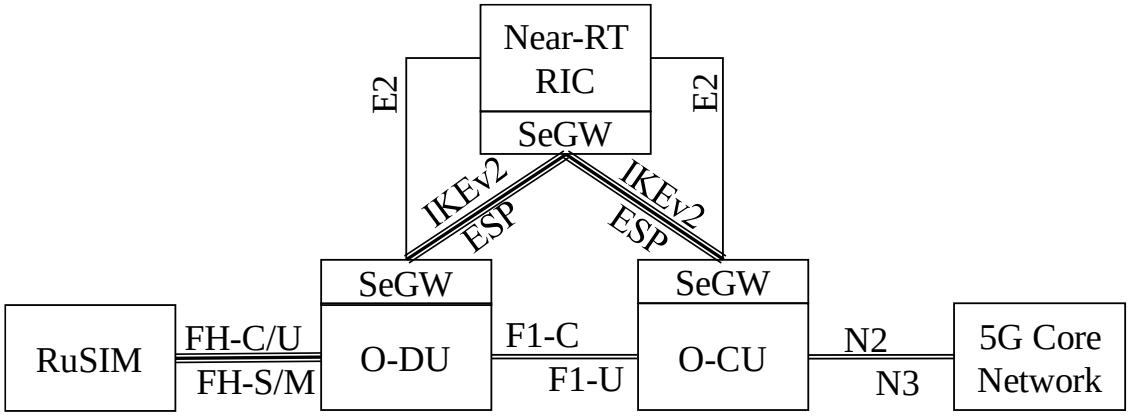
(d) 測試佈局：

見(b) 使用 RuSIM 測試

圖 38。



(a) 使用 DuSIM 與 RicSIM 測試



(b) 使用 RuSIM 測試

圖 38 控制平面資料在 E2 介面機密性保護測試示意圖

(e) 測試步驟：

(1) 在用戶設備設定支援 NEA1、NEA2、NIA1、NIA2 機密和完整性安全演算法。

(2) 在待測物 O-CU 端設定 NEA1、NIA1 機密和完整性安全演算法為最優先選擇。

(3) 採用工具分析時，開始擷取 IPsec 介面封包。

(4) 待測物的安全閘道器建立 IPsec 連線。

(5) 待測物 O-CU 與 Near-RT RIC 間可以成功透過 IPsec 建立 E2AP 連線。採用自動測試時，Near-RT RIC 需為 RicSIM。

(6) 確認 O-DU 與 Near-RT RIC 間可以成功透過 IPsec 建立 E2AP 連線，且 O-DU 與待測物 O-CU 建立 F1AP 連線。

(7) 確認待測物 O-CU 與 5GC 建立 NGAP 連線，且用戶設備註冊上 5GC。

(8) 採用工具分析時，停止擷取 IPsec 介面封包。

(9) 採用工具分析時，透過 IPsec 介面封包，確認完成 IKE-SA-INIT 和 IKE-AUTH 程序並解密檢查其中之加密演算法。採用自動測試時，透過 RicSIM 端確認。

(10) 採用工具分析時，透過 IPsec 介面封包，確認使用封裝安全承載量進行資料傳輸並解密其封包。採用自動測試時，透過 RicSIM 端確認。

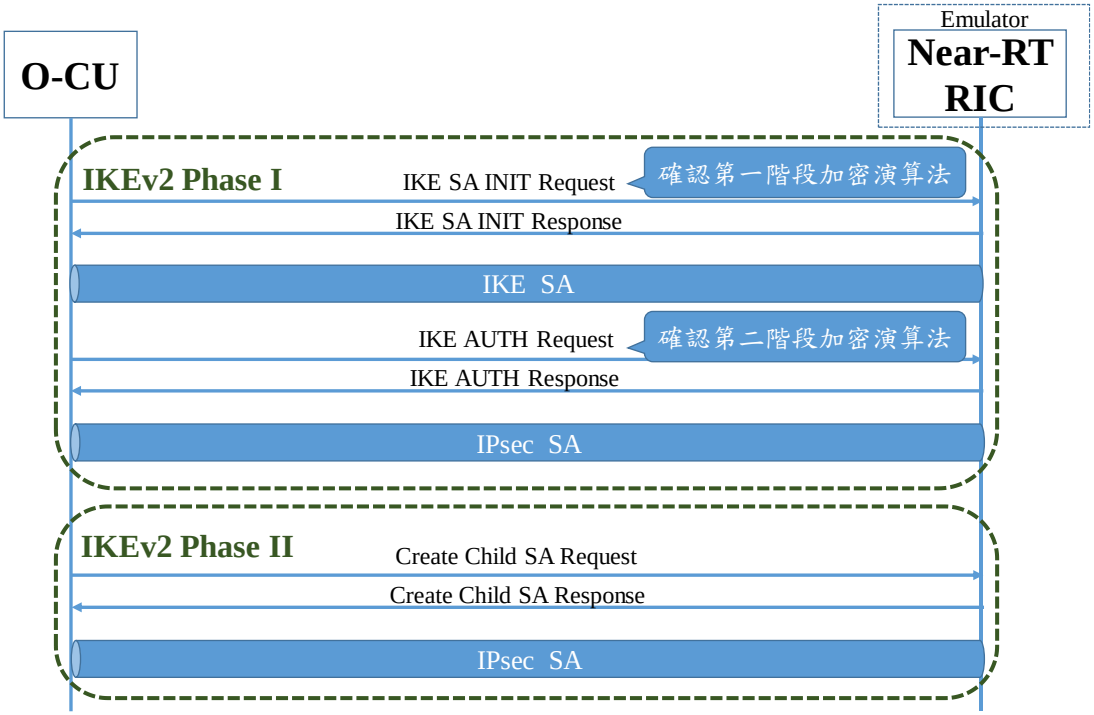


圖 39 控制平面資料在 E2 介面機密性保護測試流程圖

(f) 測試結果：

(1) 根據步驟(9)，IKE-SA-INIT 請求信令中含有 IKEv2 的第一階段加密演算法應符合以下標準。根據 3GPP REL 15 與 REL 16，其演算法支援等級分為必須支援的 Shall 和建議支援的 Should。

3GPP REL 15

i AES-CBC with 128-bit key length - Shall

ii AES-GCM with a 16 octet ICV with 128-bit key length - Shall

iii AES-GCM with a 16 octet ICV with 256-bit key length – Should

3GPP REL 16

i AES-GCM with a 16 octet ICV with 128-bit key length - Shall

ii AES-GCM with a 16 octet ICV with 256-bit key length – Should

(2) 根據步驟(9)，IKE-AUTH 是由 IKEv2 的第一階段加密演算法進行機密性保護。解密後的 IKE-AUTH 請求信令中含有 IKEv2 的第二階加密演算法應符合以下標準。其演算法支援等級分為必須支援的 Shall，標記+代表演算法強度更強。

i AES-CBC with 128-bit key length - Shall

ii AES-CBC with 256-bit key length - Shall+

iii AES-GCM with a 16 octet ICV with 128-bit key length - Shall

iv AES-GCM with a 16 octet ICV with 256-bit key length - Shall+

(3) 根據步驟(10)，封裝安全承載量資料封包是由 IKEv2 的第二階加密演算法進行機密性保護，將其解密後得到 E2AP 資料封包。

6.1.5.7 控制平面資料在 N2 介面的完整性保護

依據 TAICS TS-0035 5G 基地臺資安測試規範的 6.1.5.4 節定義之測試流程。

6.1.5.8 用戶平面資料在 N3 介面的完整性保護

依據 TAICS TS-0035 5G 基地臺資安測試規範的 6.1.5.5 節定義之測試流程。

6.1.5.9 控制平面資料在 Xn-C 介面的完整性保護

依據 TAICS TS-0035 5G 基地臺資安測試規範的 6.1.5.6 節定義之測試流程。

6.1.5.10 控制平面資料在 F1-C 介面的完整性保護

(a) 測試依據：

依據 3GPP TS 33.501 [11] 之第 5.3.9 小節與 O-RAN Security Test Specification[15]之第 6.5 小節，並參考 3GPP TS 33.210 [14] 之第 5.3.3 和 5.3.4 小節以及 3GPP TS 33.523 [9] 之第 4.2.2.1.3 小節小節。

(b) 測試目的：

驗證待測物 O-CU 的 F1-C 介面控制平面資料符合網際網路安全協定 (IPsec) 加密和認證達到完整性保護。

(c) 測試前提：

(1) 用戶設備及待測物 O-CU 間可以進行接取層安全演算法設定。

(2) 與待測物的安全閘道器間可以成功建立 IPsec 連線。

(3) 用戶設備可以採用 DuSIM 或 RuSIM 之模擬器。

i. 當用戶設備為 DuSIM 時，DuSIM 與待測物 O-CU 間可以成功透過 IPsec 建立 F1AP 連線，且 DuSIM、待測物 O-CU 及 5GC 間可以成功建立 5G 連線。

ii. 當用戶設備為 RuSIM 時，O-DU 與待測物 O-CU 間可以成功透過 IPsec 建立 F1AP 連線，且 RuSIM、O-DU、待測物 O-CU 及 5GC 間可以成功建立 5G 連線。

(4) 待測物的安全閘道器(Security Gateway, SeGW)可以支援 IKEv2，並可進行 IPsec 安全演算法設定。

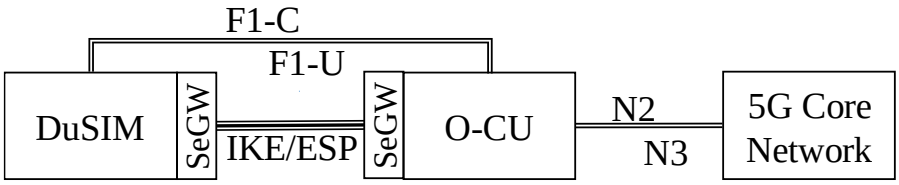
(5) 測試人員可採用分析工具或自動測試。

i. 採用工具分析時，需要擷取並解密 IPsec 介面封包，並分析 ISAKMP 與封裝安全承載內容。

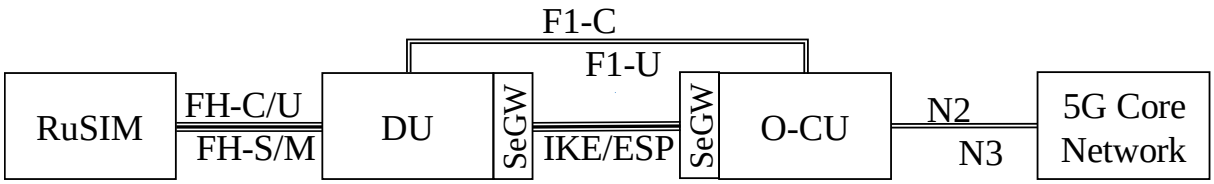
ii. 採用自動測試時，需要透過 DuSIM 的 SeGW 直接解密 IPsec 介面封包，並分析 ISAKMP 與封裝安全承載內容。

(d) 測試佈局：

見圖 40。



(a) 使用 DuSIM 測試



(b) 使用 RuSIM 測試

圖 40 控制平面資料在 F1-C 介面完整性保護測試示意圖

(e) 測試步驟：

(1) 在用戶設備設定支援 NEA1、NEA2、NIA1、NIA2 機密和完整性安全演算法。

(2) 在待測物 O-CU 端設定 NEA1、NIA1 機密和完整性安全演算法為最優先選擇。

(3) 採用工具分析時，開始擷取 IPsec 介面封包。

(4) 待測物的安全閘道器建立 IPsec 連線。

(5) 採用工具分析時，用戶設備可以採用 DuSIM 或 RuSIM 之模擬器。採用自動測試時，用戶設備只能使用 DuSIM。

i. 當用戶設備為 DuSIM 時，確認 DuSIM 與待測物 O-CU 間成功透過 IPsec 建立 F1AP 連線。

ii. 當用戶設備為 RuSIM 時，確認 RuSIM 與 O-DU 建立 Open FH 連線，且 O-DU 與待測物 O-CU 成功透過 IPsec 建立 F1AP 連線。

(6) 確認待測物 O-CU 與 5GC 建立 NGAP 連線，且用戶設備註冊上 5GC。

(7) 採用工具分析時，停止擷取 IPsec 介面封包。

(8) 採用工具分析時，透過 IPsec 介面封包，確認完成 IKE-SA-INIT 和 IKE-AUTH 程序並解密檢查其中之加密演算法。採用自動測試時，透過 DuSIM 端確認。

(9) 採用工具分析時，透過 IPsec 介面封包，確認使用封裝安全承載量進行資料傳輸並解密其封包。採用自動測試時，透過 DuSIM 端確認。

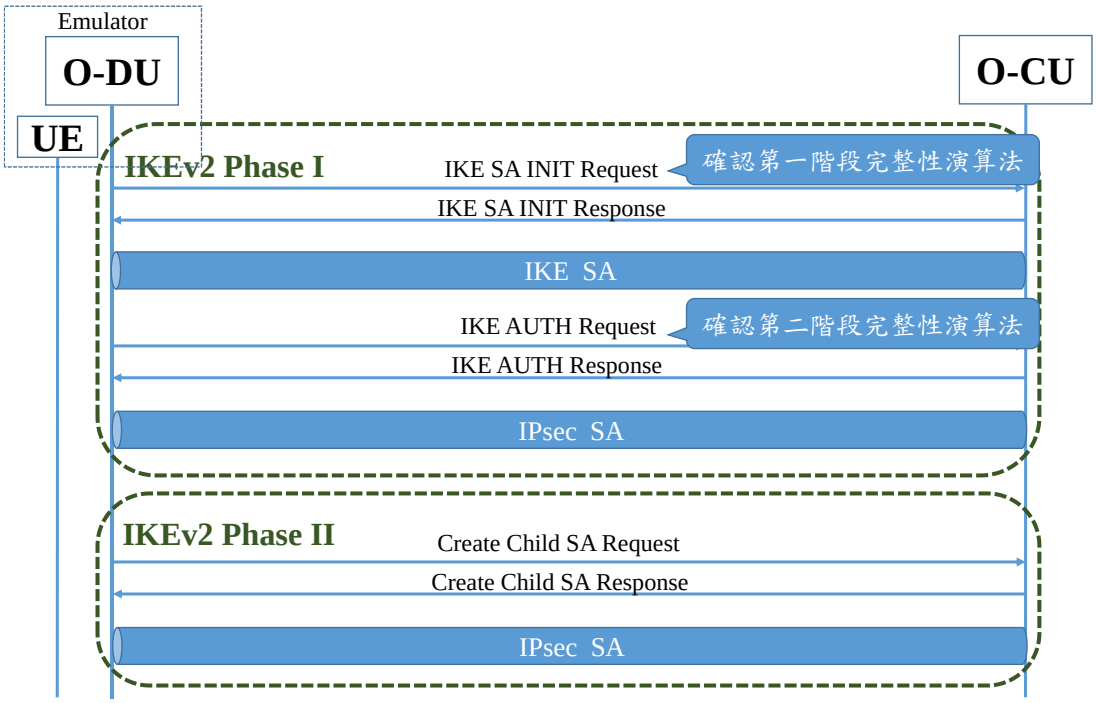


圖 41 控制平面資料在 F1-C 介面完整性保護測試流程圖

(f) 測試結果：

(1) 透過步驟(8)，IKE-SA-INIT 請求信令中含有 IKEv2 的第一階段完整性演算法需要符合以下標準。根據標準文件第 15 版和第 16 版 ，其演算法支援等級分為必須支援的 Shall 和建議支援的 Should。

第 15 版標準文件

i AUTH_HMAC_SHA1_96 - Shall

ii AUTH_HMAC_SHA2_256_128 - Shall

第 16 版標準文件

i AES-GCM with a 16 octet ICV with 128-bit key length – Shall

ii AES-GCM with a 16 octet ICV with 256-bit key length – Should

(2) 透過步驟(8)，IKE-AUTH 是由 IKEv2 的第一階段完整性演算法進行完整性保護。解密後的 IKE-AUTH 請求信令中含有 IKEv2 的第二階段完整性演算法需要符合以下標準。其演算法支援等級分為必須支援的 Shall 和建議支援的 Should，標記+代表演算法強度更強。

i AUTH_HMAC_SHA2_256_128 – Shall

ii AES_GCM with 16 octet ICV with 128-bit key length – Shall

iii AES_GCM with 16 octet ICV with 256-bit key length – Shall

iv AUTH_HMAC_SHA2_512_256 – Should

(3) 透過步驟(9)，封裝安全承載量資料封包是由 IKEv2 的第二階段完整性演算法進行完整性保護，將其解密後得到 F1AP 資料封包。

6.1.5.11 用戶平面資料在 F1-U 介面的完整性保護

(a) 測試依據：

依據 3GPP TS 33.501 [11] 之第 5.3.9 小節與 O-RAN Security Test Specification[15]之第 6.5 小節，並參考 3GPP TS 33.210 [14] 之第 5.3.3 和 5.3.4 小節以及 3GPP TS 33.523 [9]之 4.2.2.1.4 小節。

(b) 測試目的：

驗證待測物 O-CU 的 F1-C 介面用戶平面資料符合網際網路安全協定 (IPsec) 加密和認證達到完整性保護。

(c) 測試前提：

(1) 用戶設備及待測物 O-CU 間可以進行接取層安全演算法設定。

(2) 與待測物的安全閘道器間可以成功建立 IPsec 連線。

(3) 用戶設備可以採用 DuSIM 或 RuSIM 之模擬器。

i. 當用戶設備為 DuSIM 時，DuSIM 與待測物 O-CU 間可以成功透過 IPsec 建立 F1AP 連線，且 DuSIM、待測物 O-CU 及 5GC 間可以成功建立 5G 連線。

ii. 當用戶設備為 RuSIM 時，O-DU 與待測物 O-CU 間可以成功透過 IPsec 建立 F1AP 連線，且 RuSIM、O-DU、待測物 O-CU 及 5GC 間可以成功建立 5G 連線。

(4) 待測物的安全閘道器(Security Gateway, SeGW)可以支援 IKEv2，並可進行 IPsec 安全演算法設定。

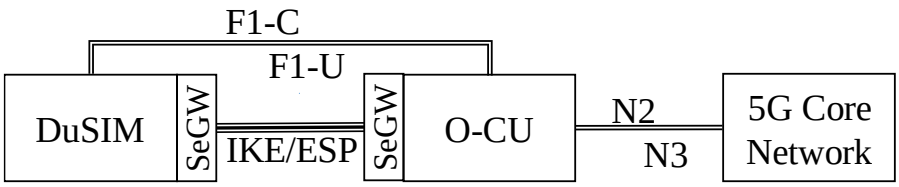
(5) 測試人員可採用分析工具或自動測試。

i. 採用工具分析時，需要擷取並解密 IPsec 介面封包，並分析 ISAKMP 與封裝安全承載內容。

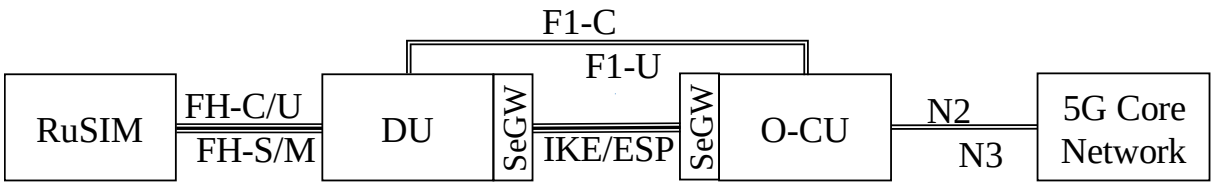
ii. 採用自動測試時，需要透過 DuSIM 的 SeGW 直接解密 IPsec 介面封包，並分析 ISAKMP 與封裝安全承載內容。

(d) 測試佈局：

見圖 42。



(a) 使用 DuSIM 測試



(b) 使用 RuSIM 測試

圖 42 用戶平面資料在 F1-U 介面完整性保護測試示意圖

(e) 測試步驟：

(1) 在用戶設備設定支援 NEA1、NEA2、NIA1、NIA2 機密和完整性安全演算法。

(2) 在待測物 O-CU 端設定 NEA1、NIA1 機密和完整性安全演算法為最優先選擇。

(3) 採用工具分析時，開始擷取 IPsec 介面封包。

(4) 待測物的安全閘道器建立 IPsec 連線。

(5) 採用工具分析時，用戶設備可以採用 DuSIM 或 RuSIM 之模擬器。採用自動測試時，用戶設備只能使用 DuSIM。

i. 當用戶設備為 DuSIM 時，確認 DuSIM 與待測物 O-CU 間成功透過 IPsec 建立 F1AP 連線。

ii. 當用戶設備為 RuSIM 時，確認 RuSIM 與 O-DU 建立 Open FH 連線，且 O-DU 與待測物 O-CU 成功透過 IPsec 建立 F1AP 連線。

(6) 確認待測物 O-CU 與 5GC 建立 NGAP 連線，且用戶設備註冊上 5GC 並收送數據資料。

(7) 採用工具分析時，停止擷取 IPsec 介面封包。

(8) 採用工具分析時，透過 IPsec 介面封包，確認完成 IKE-SA-INIT 和 IKE-AUTH 程序並解密檢查其中之加密演算法。採用自動測試時，透過 DuSIM 端確認。

(9) 採用工具分析時，透過 IPsec 介面封包，確認使用封裝安全承載量進行資料傳輸並解密其封包。採用自動測試時，透過 DuSIM 端確認。

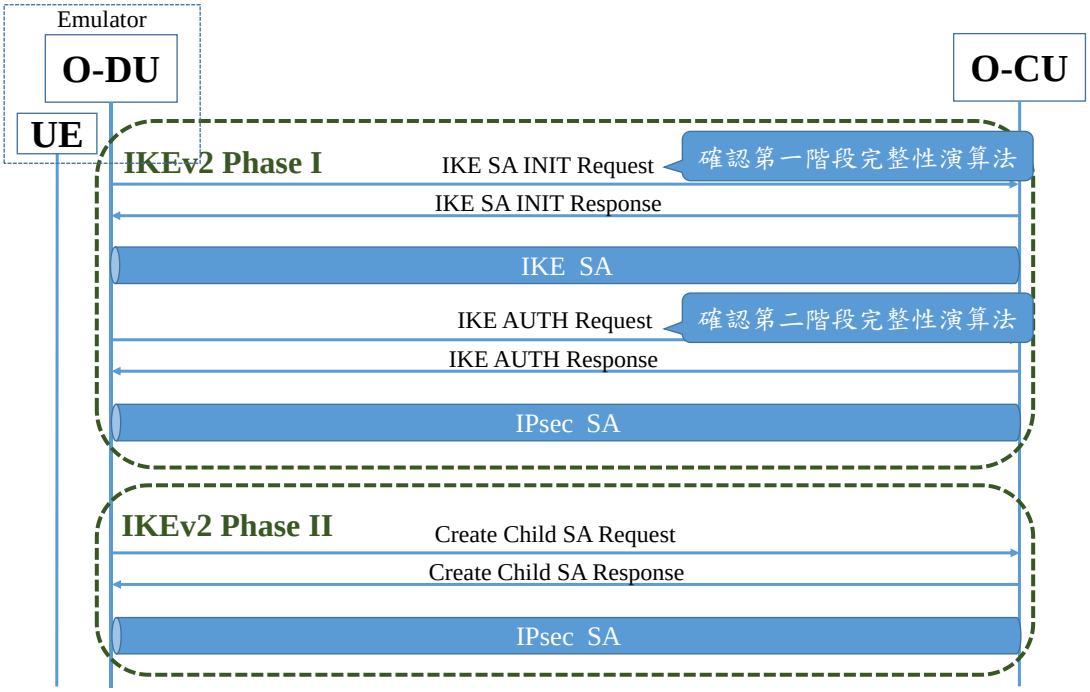


圖 43 用戶平面資料在 F1-U 介面完整性保護測試流程圖

(f) 測試結果：

(1) 透過步驟(8)，IKE-SA-INIT 請求信令中含有 IKEv2 的第一階段完整性演算法需要符合以下標準。根據標準文件第 15 版和第 16 版，其演算法支援等級分為必須支援的 Shall 和建議支援的 Should。

第 15 版標準文件

i AUTH_HMAC_SHA1_96 - Shall

ii AUTH_HMAC_SHA2_256_128 - Shall

第 16 版標準文件

i AES-GCM with a 16 octet ICV with 128-bit key length – Shall

ii AES-GCM with a 16 octet ICV with 256-bit key length – Should

(2) 透過步驟(8)，IKE-AUTH 是由 IKEv2 的第一階段完整性演算法進行完整性保護。解密後的 IKE-AUTH 請求信令中含有 IKEv2 的第二階段完整性演算法需要符合以下標準。其演算法支援等級分為必須支援的 Shall 和建議支援的 Should，標記+代表演算法強度更強。

i AUTH_HMAC_SHA2_256_128 – Shall

ii AES_GCM with 16 octet ICV with 128-bit key length – Shall

iii AES_GCM with 16 octet ICV with 256-bit key length – Shall

iv AUTH_HMAC_SHA2_512_256 – Should

(3) 透過步驟(9)，封裝安全承載量資料封包是由 IKEv2 的第二階段完整性演算法進行完整性保護，將其解密後得到 F1-U 介面之用戶平面資料封包。

6.1.5.12 控制平面資料在 E2 介面的完整性保護

(a) 測試依據：

依據 O-RAN Security Test Specification[15]之第 6.5 和 13.2 小節，並參考 O-RAN Security Protocols Specification[19]之第 2.2 小節與 3GPP TS 33.210 [14] 之第 5.3.3 和 5.3.4 小節。

(b) 測試目的：

驗證待測物 O-CU 的 E2 介面控制平面資料符合網際網路安全協定 (IPsec) 加密和認證達到完整性保護。

(c) 測試前提：

(1) 用戶設備及待測物 O-CU 間可以進行接取層安全演算法設定。

(2) 與待測物的安全閘道器間可以成功建立 IPsec 連線。

(3) 待測物 O-CU 與 Near-RT RIC 間可以成功透過 IPsec 建立 E2AP 連線。

(4) 確認 O-DU 與 Near-RT RIC 間可以成功透過 IPsec 建立 E2AP 連線，且 O-DU、待測物 O-CU 及 5GC 間可以成功建立 5G 連線。採用自動測試時，Near-RT RIC 需為 RicSIM。

(5) 待測物的安全閘道器(Security Gateway, SeGW)可以支援 IKEv2，並可進行 IPsec 安全演算法設定。

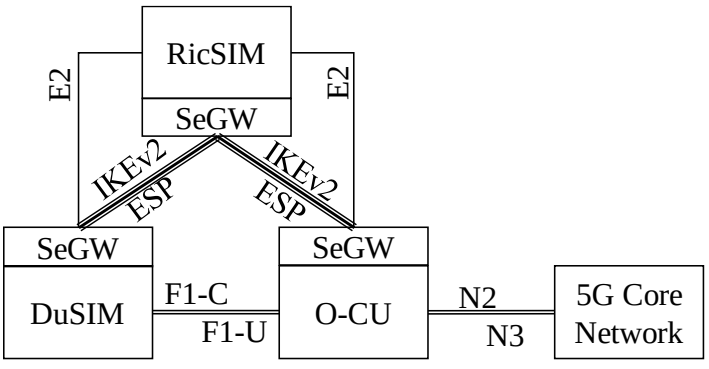
(6) 測試人員可採用分析工具或自動測試。

i. 採用工具分析時，需要擷取並解密 IPsec 介面封包，並分析 ISAKMP 與封裝安全承載內容。

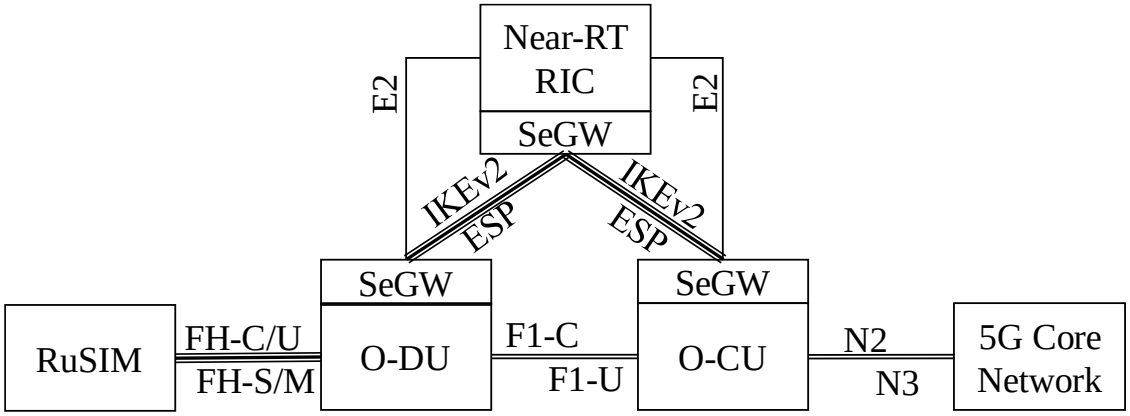
ii. 採用自動測試時，需要透過 RicSIM 之模擬器的 SeGW 直接解密 IPsec 介面封包，並分析 ISAKMP 與封裝安全承載內容。

(d) 測試佈局：

見圖 44。



(a) 使用 DuSIM 與 RicSIM 測試



(b) 使用 RuSIM 測試

圖 44 控制平面資料在 E2 介面完整性保護測試示意圖

(e) 測試步驟：

(1) 在用戶設備設定支援 NEA1、NEA2、NIA1、NIA2 機密和完整性安全演算法。

(2) 在待測物 O-CU 端設定 NEA1、NIA1 機密和完整性安全演算法為最優先選擇。

(3) 採用工具分析時，開始擷取 IPsec 介面封包。

(4) 待測物的安全閘道器建立 IPsec 連線。

(5) 待測物 O-CU 與 Near-RT RIC 間可以成功透過 IPsec 建立 E2AP 連線。採用自動測試時，Near-RT RIC 需為 RicSIM。

(6) 確認 O-DU 與 Near-RT RIC 間可以成功透過 IPsec 建立 E2AP 連線，且 O-DU 與待測物 O-CU 建立 F1AP 連線。

(7) 確認待測物 O-CU 與 5GC 建立 NGAP 連線，且用戶設備註冊上 5GC。

(8) 採用工具分析時，停止擷取 IPsec 介面封包。

(9) 採用工具分析時，透過 IPsec 介面封包，確認完成 IKE-SA-INIT 和 IKE-AUTH 程序並解密檢查其中之加密演算法。採用自動測試時，透過 RicSIM 端確認。

(10) 採用工具分析時，透過 IPsec 介面封包，確認使用封裝安全承載量進行資料傳輸並解密其封包。採用自動測試時，透過 RicSIM 端確認。

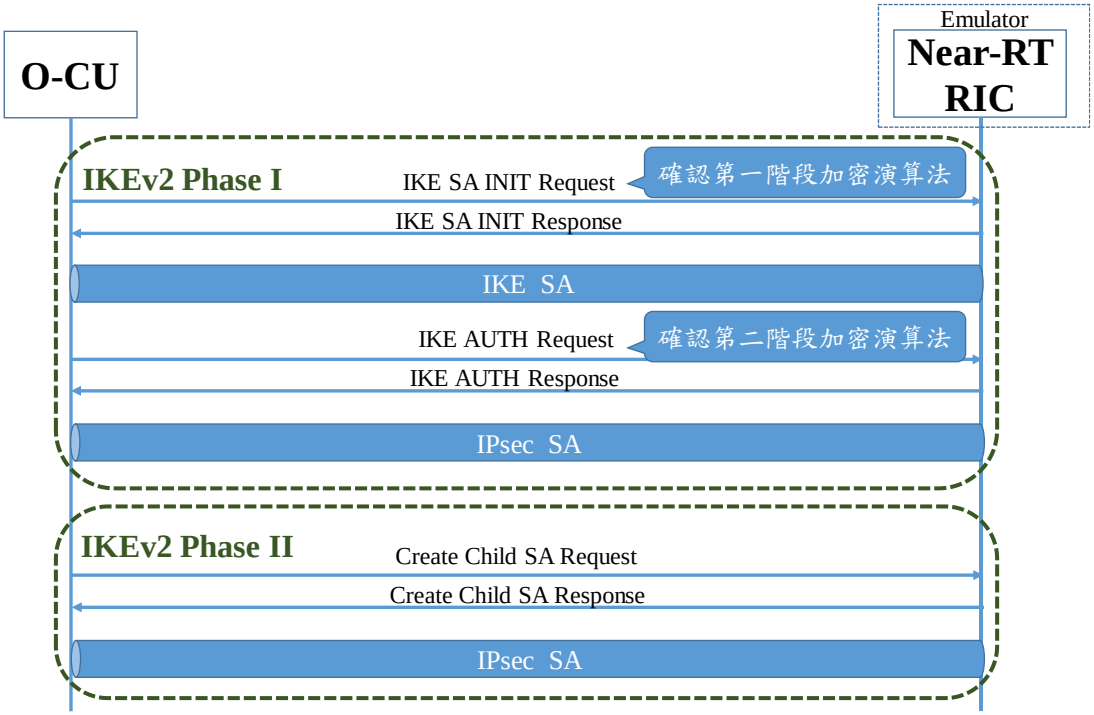


圖 45 控制平面資料在 E2 介面完整性保護測試流程圖

(f) 測試結果：

(1) 透過步驟(9)，IKE-SA-INIT 請求信令中含有 IKEv2 的第一階段完整性演算法需要符合以下標準。根據標準文件第 15 版和第 16 版 ，其演算法支援等級分為必須支援的 Shall 和建議支援的 Should。

第 15 版標準文件

i. AUTH_HMAC_SHA1_96 - Shall

ii. AUTH_HMAC_SHA2_256_128 - Shall

第 16 版標準文件

i. AES-GCM with a 16 octet ICV with 128-bit key length – Shall

ii. AES-GCM with a 16 octet ICV with 256-bit key length – Should

(2) 透過步驟(9)，IKE-AUTH 是由 IKEv2 的第一階段完整性演算法進行完整性保護。解密後的 IKE-AUTH 請求信令中含有 IKEv2 的第二階段完整性演算法需要符合以下標準。其演算法支援等級分為必須支援的 Shall 和建議支援的 Should，標記+代表演算法強度更強。

i. AUTH_HMAC_SHA2_256_128 – Shall

ii. AES_GCM with 16 octet ICV with 128-bit key length – Shall

iii. AES_GCM with 16 octet ICV with 256-bit key length – Shall

iv. AUTH_HMAC_SHA2_512_256 – Should

(3) 透過步驟(10)，封裝安全承載量資料封包是由 IKEv2 的第二階段完整性演算法進行完整性保護，將其解密後得到 E2AP 資料封包。

6.1.6 O-CU 介面功能安全性檢測

6.1.6.1 通用封包無線服務隧道協定-用戶平面的過濾功能測試

依據 TAICS TS-0035 5G 基地臺資安測試規範的 6.1.6.1 節定義之測試流程。

6.1.6.2 N2 介面的模糊測試(非必測項目)

依據 TAICS TS-0035 5G 基地臺資安測試規範的 6.1.6.2 節定義之測試流程。

6.1.6.3 N3 介面的模糊測試(非必測項目)

依據 TAICS TS-0035 5G 基地臺資安測試規範的 6.1.6.3 節定義之測試流程。

6.1.6.4 Xn-C 介面的模糊測試(非必測項目)

依據 TAICS TS-0035 5G 基地臺資安測試規範的 6.1.6.4 節定義之測試流程。

6.1.6.5 F1-C 介面的模糊測試(非必測項目)

(a) 測試依據：

參考 O-RAN Security Test Specification[15]之第 7.4 小節與 3GPP TS 33.117[2]之第 4.4.4 小節。

(b) 測試目的：

驗證待測物 O-CU 的 F1-C 介面能夠適當處裡非預期的 F1AP 封包。

(c) 測試前提：

(1) O-DU 模糊測試器可成功與待測物 O-CU 以及 5GC 建立 5G 連線。

(2) 測試人員可採用分析工具或自動測試。

i. 採用工具分析時，需要擷取 F1AP 封包並分析其封包內容。

ii. 採用自動測試時，需要透過 O-DU 模糊測試器分析 F1AP 封包內容。

(d) 測試佈局：

見圖 46。

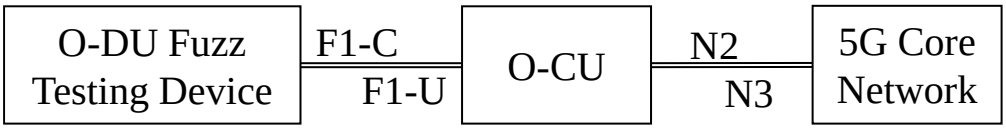


圖 46 F1-C 介面的模糊測試示意圖

(e) 測試步驟：

(1) 採用工具分析時，開始擷取 F1-C 介面封包。

(2) O-DU 模糊測試器可成功與待測物 O-CU 建立 F1AP 連線。

(3) O-DU 模糊測試器對待測物 O-CU 發送非預期的 F1AP 封包。

(4) 採用工具分析時，停止擷取 F1AP 封包。

(5) 採用工具分析時，透過 F1AP 封包，確認待測物 O-CU 是否捨棄非預期的 F1AP 封包亦或回覆 F1AP 封包錯誤。採用自動測試時，由 O-DU 模糊測試器確認。

(6) 應用協定介面封包，O-DU 模糊測試器重新與待測物 O-CU 建立 F1AP 連線。

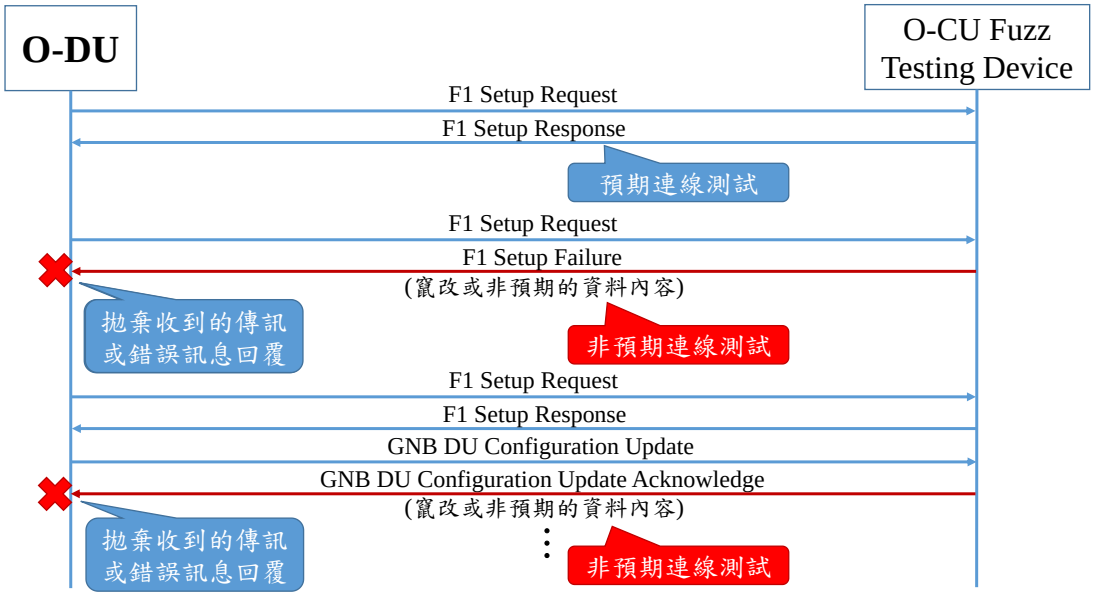


圖 47 F1-C 介面的模糊測試流程圖

(f) 測試結果：

(1) 根據步驟(5)和(6)，O-CU 捨棄非預期的 F1AP 封包或回覆 F1AP 封包錯誤，並持續與建立 F1AP 連線。

6.1.7 O-DU 安全通道檢測

6.1.7.1 控制平面資料在 F1-C 介面的機密性保護

(a) 測試依據：

依據 3GPP TS 33.501 [11] 之第 5.3.9 小節與 O-RAN Security Test Specification[15]之第 6.5 小節，並參考 3GPP TS 33.210 [14] 之第 5.3.3 和 5.3.4 小節以及 3GPP TS 33.523 [9]之 7.2.2.1.1 小節。

(b) 測試目的：

驗證待測物 O-DU 的 F1-C 介面控制平面資料符合網際網路安全協定 (IPsec) 加密和認證達到機密性保護。

(c) 測試前提：

(1) 用戶設備及 O-CU 間可以進行接取層安全演算法設定。

(2) 與待測物的安全閘道器可以成功建立 IPsec 連線。

(3) 用戶設備採用 RuSIM 之模擬器時，待測物 O-DU 與 O-CU 間可以成功透過 IPsec 建立 F1AP 連線，且 RuSIM、待測物 O-DU、O-CU 及 5GC 間可以成功建立 5G 連線。採用自動測試時，5GC 與 O-CU 需為 5gcuSIM 之模擬器，待測物 O-DU 與 5gcuSIM 間可以成功透過 IPsec 建立 F1AP 連線，RuSIM、待測物 O-DU、5gcuSIM 間可以成功建立 5G 連線。

(4) 待測物的安全閘道器(Security Gateway, SeGW)都可以支援 IKEv2，並可進行 IPsec 安全演算法設定。

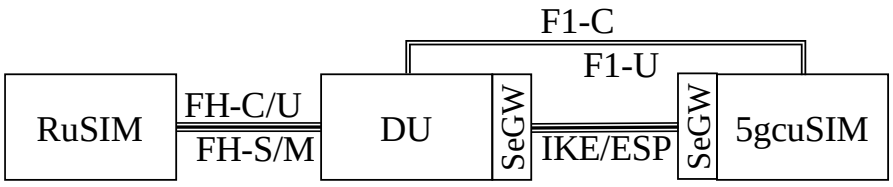
(5) 測試人員可採用分析工具或自動測試。

i. 採用工具分析時，需要擷取並解密 IPsec 介面封包，並分析 ISAKMP 與封裝安全承載內容。

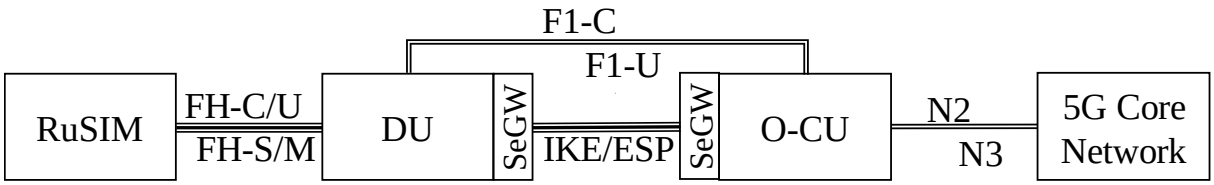
ii. 採用自動測試時，需要透過 5gcuSIM 的 SeGW 直接解密 IPsec 介面封包，並分析 ISAKMP 與封裝安全承載內容。

(d) 測試佈局：

見圖 48。



(a) 使用 RuSIM 與 5gcuSIM 測試



(b) 使用 RuSIM 測試

圖 48 控制平面資料在 F1-C 介面機密性保護測試示意圖

(e) 測試步驟：

(1) 在用戶設備設定支援 NEA1、NEA2、NIA1、NIA2 機密和完整性安全演算法。

(2) 在 O-CU 端設定 NEA1、NIA1 機密和完整性安全演算法為最優先選擇。

(3) 採用工具分析時，開始擷取 IPsec 介面封包。

(4) 與待測物的安全閘道器建立 IPsec 連線。

(5) 確認待測物 O-DU 與 O-CU 或 5gcuSIM 間成功透過 IPsec 建立 F1AP 連線。

(6) 確認用戶設備註冊上 5GC 或 5gcuSIM。

(7) 採用工具分析時，停止擷取 IPsec 介面封包。

(8) 採用工具分析時，透過 IPsec 介面封包，確認完成 IKE-SA-INIT 和 IKE-AUTH 程序並解密檢查其中之加密演算法。採用自動測試時，透過 5gcuSIM 端確認。

(9) 採用工具分析時，透過 IPsec 介面封包，確認使用封裝安全承載量進行資料傳輸並解密其封包。採用自動測試時，透過 5gcuSIM 端確認。

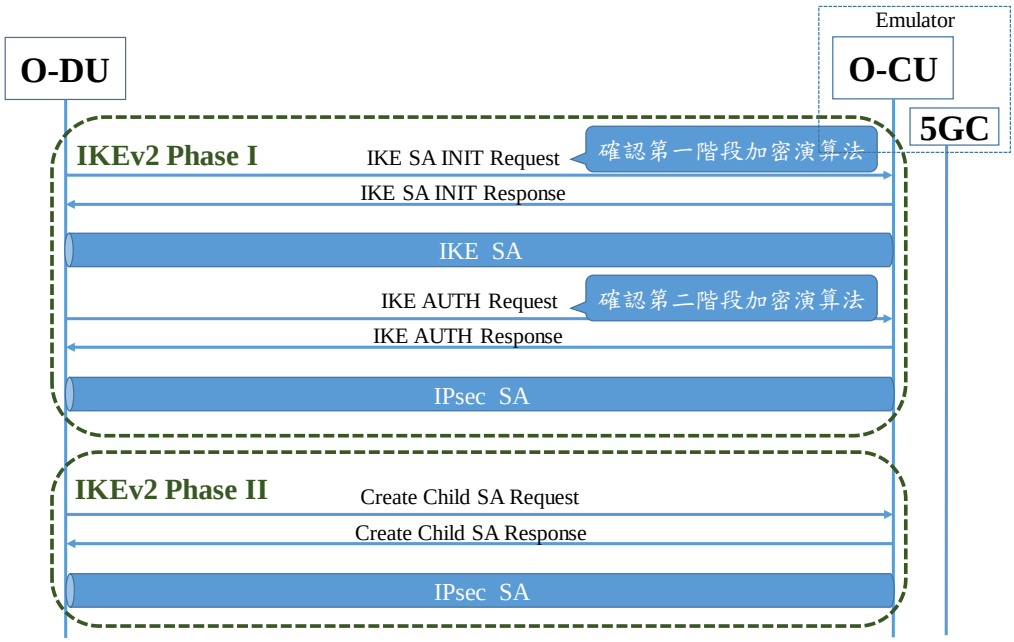


圖 49 控制平面資料在 F1-C 介面機密性保護測試流程圖

(f) 測試結果：

(1) 根據步驟(8)，IKE-SA-INIT 請求信令中含有 IKEv2 的第一階段加密演算法應符合以下標準。根據 3GPP REL 15 與 REL 16，其演算法支援等級分為必須支援的 Shall 和建議支援的 Should。

3GPP REL 15

i AES-CBC with 128-bit key length - Shall

ii AES-GCM with a 16 octet ICV with 128-bit key length - Shall

iii AES-GCM with a 16 octet ICV with 256-bit key length – Should

3GPP REL 16

i AES-GCM with a 16 octet ICV with 128-bit key length - Shall

ii AES-GCM with a 16 octet ICV with 256-bit key length – Should

(2) 根據步驟(8)，IKE-AUTH 是由 IKEv2 的第一階段加密演算法進行機密性保護。解密後的 IKE-AUTH 請求信令中含有 IKEv2 的第二階加密演算法應符合以下標準。其演算法支援等級分為必須支援的 Shall，標記+代表演算法強度更強。

i AES-CBC with 128-bit key length - Shall

ii AES-CBC with 256-bit key length - Shall+

iii AES-GCM with a 16 octet ICV with 128-bit key length - Shall

iv AES-GCM with a 16 octet ICV with 256-bit key length - Shall+

(3) 根據步驟(9)，封裝安全承載量資料封包是由 IKEv2 的第二階加密演算法進行機密性保護，將其解密後得到 F1AP 資料封包。

6.1.7.2 控制平面資料在 F1-U 介面的機密性保護

(a) 測試依據：

依據 3GPP TS 33.501 [11] 之第 5.3.9 小節與 O-RAN Security Test Specification[15]之第 6.5 小節，並參考 3GPP TS 33.210 [14] 之第 5.3.3 和 5.3.4 小節以及 3GPP TS 33.523 [9]之 7.2.2.1.3 小節。

(b) 測試目的：

驗證待測物 O-DU 的 F1-U 介面控制平面資料符合網際網路安全協定 (IPsec) 加密和認證達到機密性保護。

(c) 測試前提：

(1) 用戶設備及 O-CU 間可以進行接取層安全演算法設定。

(2) 與待測物的安全閘道器可以成功建立 IPsec 連線。

(3) 用戶設備採用 RuSIM 之模擬器時，待測物 O-DU 與 O-CU 間可以成功透過 IPsec 建立 F1AP 連線，且 RuSIM、待測物 O-DU、O-CU 及 5GC 間可以成功建立 5G 連線。採用自動測試時，5GC 與 O-CU 需為 5gcuSIM 之模擬器，待測物 O-DU 與 5gcuSIM 間可以成功透過 IPsec 建立 F1AP 連線，RuSIM、O-DU、5gcuSIM 間可以成功建立 5G 連線。

(4) 待測物的安全閘道器(Security Gateway, SeGW)都可以支援 IKEv2，並可進行 IPsec 安全演算法設定。

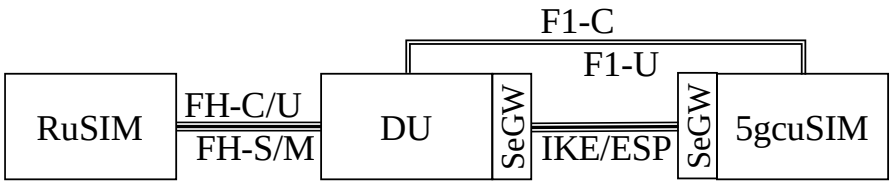
(5) 測試人員可採用分析工具或自動測試。

i. 採用工具分析時，需要擷取並解密 IPsec 介面封包，並分析 ISAKMP 與封裝安全承載內容。

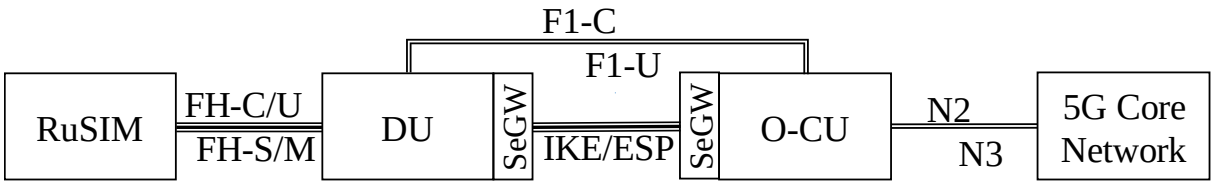
ii. 採用自動測試時，需要透過 5gcuSIM 的 SeGW 直接解密 IPsec 介面封包，並分析 ISAKMP 與封裝安全承載內容。

(d) 測試佈局：

見圖 50。



(a) 使用 RuSIM 與 5gcuSIM 測試



(b) 使用 RuSIM 測試

圖 50 控制平面資料在 F1-C 介面機密性保護測試示意圖

(e) 測試步驟：

(1) 在用戶設備設定支援 NEA1、NEA2、NIA1、NIA2 機密和完整性安全演算法。

(2) 在 O-CU 端設定 NEA1、NIA1 機密和完整性安全演算法為最優先選擇。

(3) 採用工具分析時，開始擷取 IPsec 介面封包。

(4) 與待測物的安全閘道器建立 IPsec 連線。

(5) 採用工具分析時，確認待測物 O-DU 與 O-CU 或 5gcuSIM 間成功透過 IPsec 建立 F1AP 連線。

(6) 確認用戶設備註冊上 5GC 或 5gcuSIM。

(7) 採用工具分析時，停止擷取 IPsec 介面封包。

(8) 採用工具分析時，透過 IPsec 介面封包，確認完成 IKE-SA-INIT 和 IKE-AUTH 程序並解密檢查其中之加密演算法。採用自動測試時，透過 5gcuSIM 端確認。

(9) 採用工具分析時，透過 IPsec 介面封包，確認使用封裝安全承載量進行資料傳輸並解密其封包。採用自動測試時，透過 5gcuSIM 端確認。

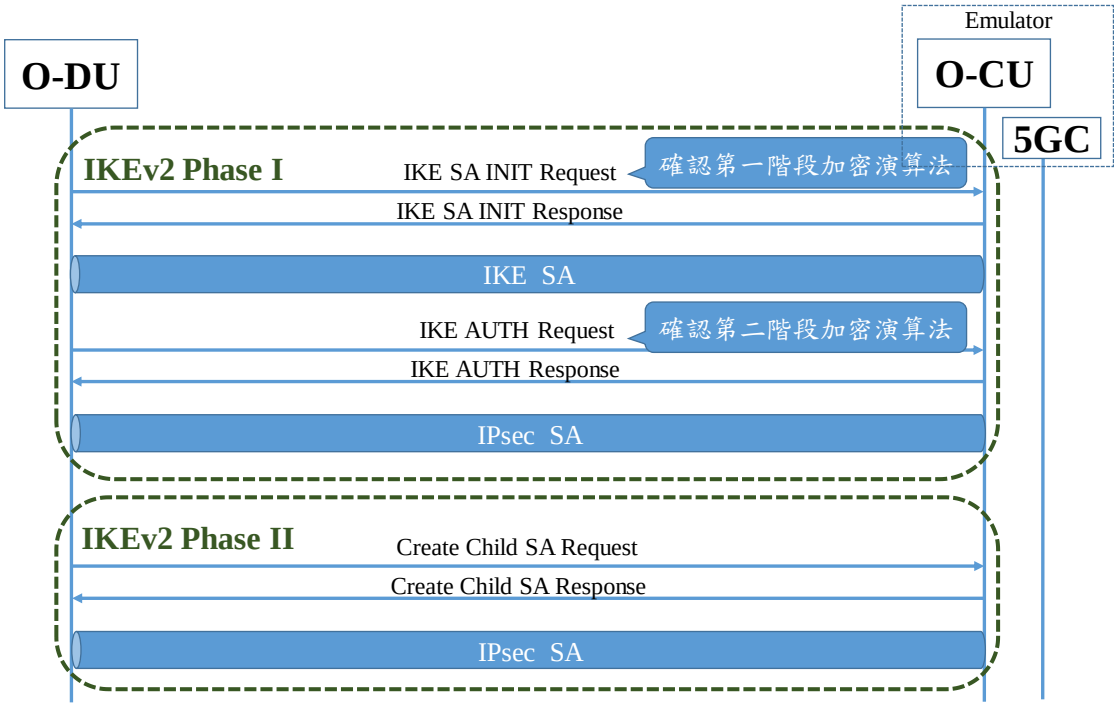


圖 51 控制平面資料在 F1-C 介面機密性保護測試流程圖

(f) 測試結果：

(1) 根據步驟(8)，IKE-SA-INIT 請求信令中含有 IKEv2 的第一階段加密演算法應符合以下標準。根據 3GPP REL 15 與 REL 16，其演算法支援等級分為必須支援的 Shall 和建議支援的 Should。

3GPP REL 15

i AES-CBC with 128-bit key length - Shall

ii AES-GCM with a 16 octet ICV with 128-bit key length - Shall

iii AES-GCM with a 16 octet ICV with 256-bit key length – Should

3GPP REL 16

i AES-GCM with a 16 octet ICV with 128-bit key length - Shall

ii AES-GCM with a 16 octet ICV with 256-bit key length – Should

(2) 根據步驟(8)，IKE-AUTH 是由 IKEv2 的第一階段加密演算法進行機密性保護。解密後的 IKE-AUTH 請求信令中含有 IKEv2 的第二階加密演算法應符合以下標準。其演算法支援等級分為必須支援的 Shall，標記+代表演算法強度更強。

i AES-CBC with 128-bit key length - Shall

ii AES-CBC with 256-bit key length - Shall+

iii AES-GCM with a 16 octet ICV with 128-bit key length - Shall

iv AES-GCM with a 16 octet ICV with 256-bit key length - Shall+

(3) 根據步驟(9)，封裝安全承載量資料封包是由 IKEv2 的第二階加密演算法進行機密性保護，將其解密後得到 F1-U 資料封包。

6.1.7.3 控制平面資料在 E2 介面的機密性保護

(a) 測試依據：

依據 O-RAN Security Test Specification [15]之 6.5 和 13.2 小節，並參考 O-RAN Security Protocols Specification [19]之第 2.2 小節與 3GPP TS 33.210 [14] 之第 5.3.3 和 5.3.4 小節。

(b) 測試目的：

驗證待測物 O-DU 的 E2 介面控制平面資料符合網際網路安全協定 (IPsec) 加密和認證達到機密性保護。

(c) 測試前提：

(1) 用戶設備及 O-CU 間可以進行接取層安全演算法設定。

(2) 與待測物的安全閘道器間可以成功建立 IPsec 連線。

(3) 用戶設備可以採用 RuSIM，待測物 O-DU 與 Near-RT RIC 間可以成功透過 IPsec 建立 E2AP 連線。採用自動測試時，Near-RT RIC 需為 RicSIM 之模擬器，待測物 O-DU 與 RicSIM 間可以成功透過 IPsec 建立 E2AP 連線，RuSIM、待測物 O-DU、O-CU 與 5GC 間可以成功建立 5G 連線。

(4) 待測物的安全閘道器(Security Gateway, SeGW)可以支援 IKEv2，並可進行 IPsec 安全演算法設定。

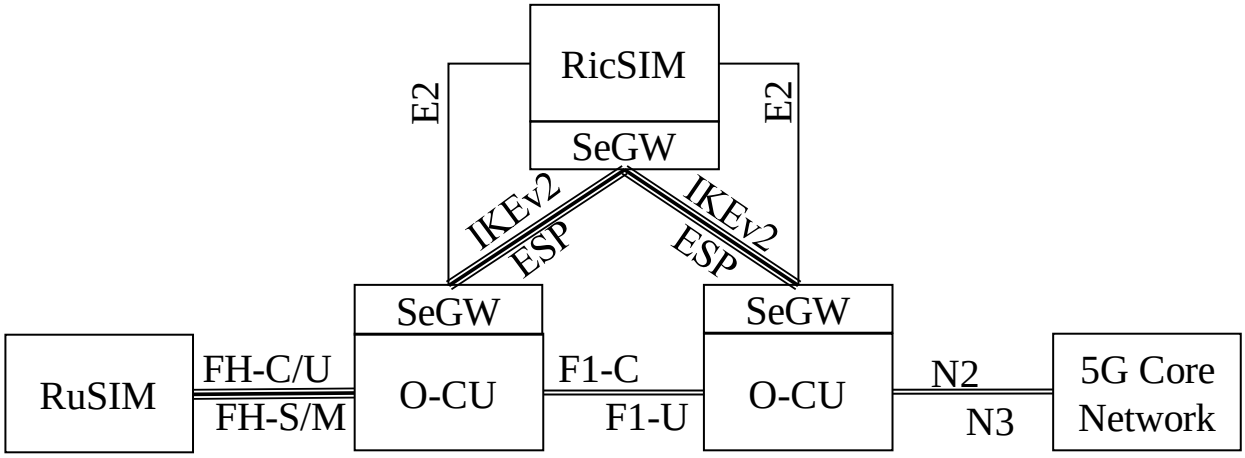
(5) 測試人員可採用分析工具或自動測試。

i. 採用工具分析時，需要擷取並解密 IPsec 介面封包，並分析 ISAKMP 與封裝安全承載內容。

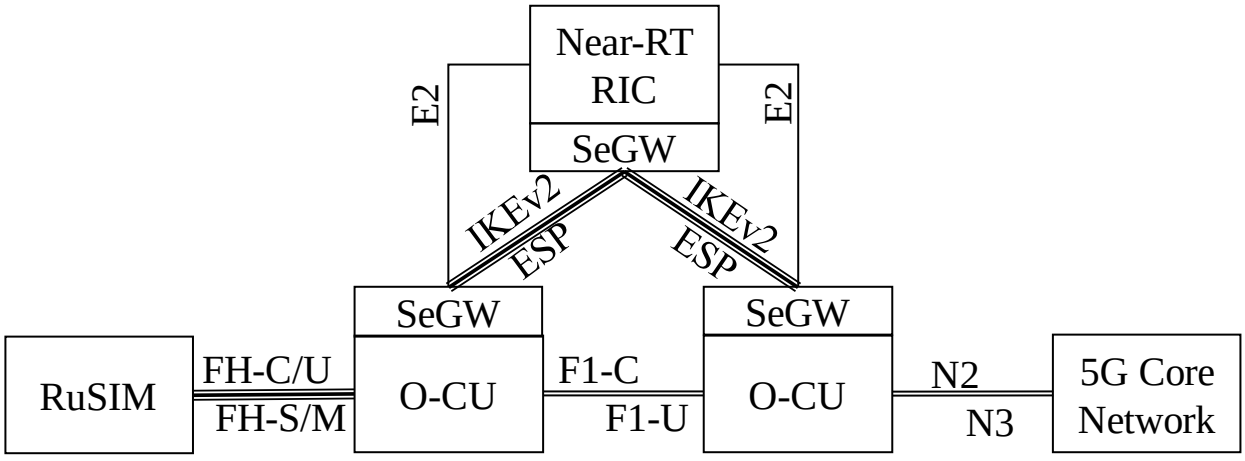
ii. 採用自動測試時，需要透過 RicSIM 的 SeGW 直接解密 IPsec 介面封包，並分析 ISAKMP 與封裝安全承載內容。

(d) 測試佈局：

見圖 52。



(a) 使用 RuSIM 與 RicSIM 測試



(b) 使用 RuSIM 測試

圖 52 控制平面資料在 E2 介面機密性保護測試示意圖

(e) 測試步驟：

(1) 在用戶設備設定支援 NEA1、NEA2、NIA1、NIA2 機密和完整性安全演算法。

(2) 在 O-CU 端設定 NEA1、NIA1 機密和完整性安全演算法為最優先選擇。

(3) 採用工具分析時，開始擷取 IPsec 介面封包。

(4) 待測物的安全閘道器建立 IPsec 連線。

(5) O-CU 與 Near-RT RIC 間可以成功透過 IPsec 建立 E2AP 連線。

(6) 確認待測物 O-DU 與 Near-RT RIC 間可以成功透過 IPsec 建立 E2AP 連線，且待測物 O-DU 與 O-CU 建立 F1AP 連線。採用自動測試時，Near-RT RIC 需為 RicSIM。

(7) 確認 O-CU 與 5GC 建立 NGAP 連線，且用戶設備註冊上 5GC。

(8) 採用工具分析時，停止擷取 IPsec 介面封包。

(9) 採用工具分析時，透過 IPsec 介面封包，確認完成 IKE-SA-INIT 和 IKE-AUTH 程序並解密檢查其中之加密演算法。採用自動測試時，透過 RicSIM 端確認。

(10) 採用工具分析時，透過 IPsec 介面封包，確認使用封裝安全承載量進行資料傳輸並解密其封包。採用自動測試時，透過 RicSIM 端確認。

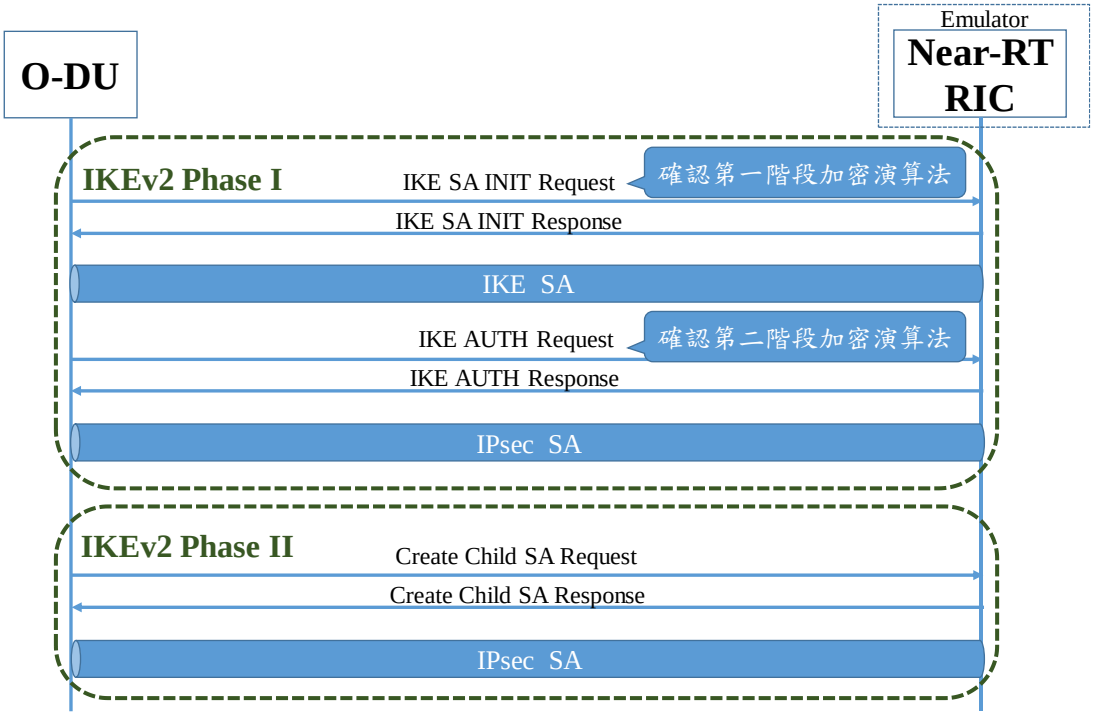


圖 53 控制平面資料在 E2 介面機密性保護測試流程圖

(f) 測試結果：

(1) 根據步驟(9)，IKE-SA-INIT 請求信令中含有 IKEv2 的第一階段加密演算法應符合以下標準。根據 3GPP REL 15 與 REL 16，其演算法支援等級分為必須支援的 Shall 和建議支援的 Should。

3GPP REL 15

i AES-CBC with 128-bit key length - Shall

ii AES-GCM with a 16 octet ICV with 128-bit key length - Shall

iii AES-GCM with a 16 octet ICV with 256-bit key length – Should

3GPP REL 16

i AES-GCM with a 16 octet ICV with 128-bit key length - Shall

ii AES-GCM with a 16 octet ICV with 256-bit key length – Should

(2) 根據步驟(9)，IKE-AUTH 是由 IKEv2 的第一階段加密演算法進行機密性保護。解密後的 IKE-AUTH 請求信令中含有 IKEv2 的第二階加密演算法應符合以下標準。其演算法支援等級分為必須支援的 Shall，標記+代表演算法強度更強。

i AES-CBC with 128-bit key length - Shall

ii AES-CBC with 256-bit key length - Shall+

iii AES-GCM with a 16 octet ICV with 128-bit key length - Shall

iv AES-GCM with a 16 octet ICV with 256-bit key length - Shall+

(3) 根據步驟(10)，封裝安全承載量資料封包是由 IKEv2 的第二階加密演算法進行機密性保護，將其解密後得到 E2AP 資料封包。

6.1.7.4 控制平面資料在 F1-C 介面的完整性保護

(a) 測試依據：

依據 3GPP TS 33.501 [11] 之第 5.3.9 小節與 O-RAN Security Test Specification[15]之第 6.5 小節，並參考 3GPP TS 33.210 [14] 之第 5.3.3 和 5.3.4 小節以及 3GPP TS 33.523 [9]之 7.2.2.1.2 小節。

(b) 測試目的：

驗證待測物 O-DU 的 F1-C 介面控制平面資料符合網際網路安全協定 (IPsec) 加密和認證達到完整性保護。

(c) 測試前提：

(1) 用戶設備及 O-CU 間可以進行接取層安全演算法設定。

(2) 與待測物的安全閘道器可以成功建立 IPsec 連線。

(3) 用戶設備採用 RuSIM 之模擬器時，待測物 O-DU 與 O-CU 間可以成功透過 IPsec 建立 F1AP 連線，且 RuSIM、待測物 O-DU、O-CU 及 5GC 間可以成功建立 5G 連線。採用自動測試時，5GC 與 O-CU 需為 5gcuSIM 之模擬器，待測物 O-DU 與 5gcuSIM 間可以成功透過 IPsec 建立 F1AP 連線，RuSIM、待測物 O-DU、5gcuSIM 間可以成功建立 5G 連線。

(4) 待測物的安全閘道器(Security Gateway, SeGW)都可以支援 IKEv2，並可進行 IPsec 安全演算法設定。

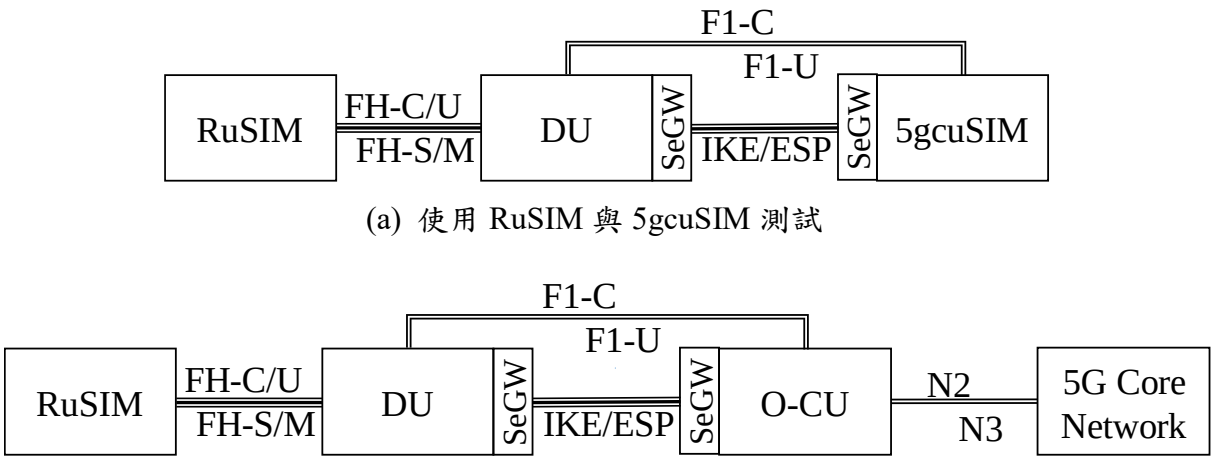
(5) 測試人員可採用分析工具或自動測試。

i. 採用工具分析時，需要擷取並解密 IPsec 介面封包，並分析 ISAKMP 與封裝安全承載內容。

ii. 採用自動測試時，需要透過 5gcuSIM 的 SeGW 直接解密 IPsec 介面封包，並分析 ISAKMP 與封裝安全承載內容。

(d) 測試佈局：

見圖 54。



(a) 使用 RuSIM 與 5gcuSIM 測試

(b) 使用 RuSIM 測試

圖 54 控制平面資料在 F1-C 介面機密性保護測試示意圖

(e) 測試步驟：

(1) 在用戶設備設定支援 NEA1、NEA2、NIA1、NIA2 機密和完整性安全演算法。

(2) 在 O-CU 端設定 NEA1、NIA1 機密和完整性安全演算法為最優先選擇。

(3) 採用工具分析時，開始擷取 IPsec 介面封包。

(4) 與待測物的安全閘道器建立 IPsec 連線。

(5) 採用工具分析時，確認待測物 O-DU 與 O-CU 或 5gcuSIM 間成功透過 IPsec 建立 F1AP 連線。

(6) 確認用戶設備註冊上 5GC 或 5gcuSIM。

(7) 採用工具分析時，停止擷取 IPsec 介面封包。

(8) 採用工具分析時，透過 IPsec 介面封包，確認完成 IKE-SA-INIT 和 IKE-AUTH 程序並解密檢查其中之加密演算法。採用自動測試時，透過 5gcuSIM 端確認。

(9) 採用工具分析時，透過 IPsec 介面封包，確認使用封裝安全承載量進行資料傳輸並解密其封包。採用自動測試時，透過 5gcuSIM 端確認。

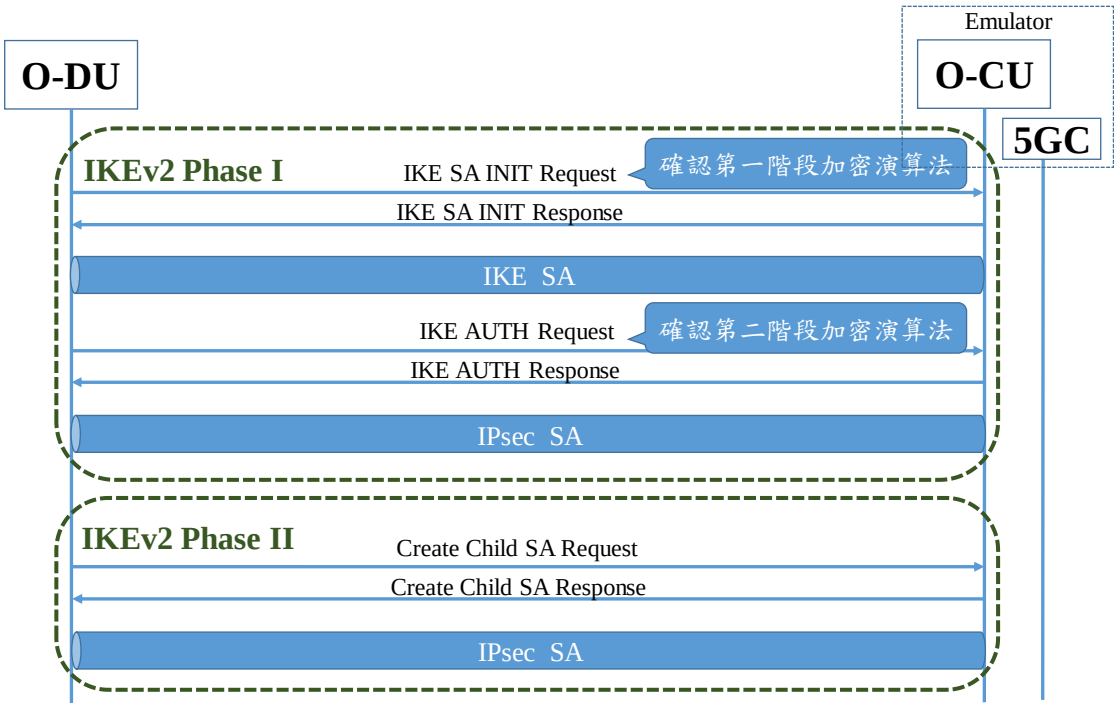


圖 55 控制平面資料在 F1-C 介面機密性保護測試流程圖

(f) 測試結果：

(1) 透過步驟(8)，IKE-SA-INIT 請求信令中含有 IKEv2 的第一階段完整性演算法需要符合以下標準。根據標準文件第 15 版和第 16 版，其演算法支援等級分為必須支援的 Shall 和建議支援的 Should。

第 15 版標準文件

i AUTH_HMAC_SHA1_96 - Shall

ii AUTH_HMAC_SHA2_256_128 - Shall

第 16 版標準文件

i AES-GCM with a 16 octet ICV with 128-bit key length – Shall

ii AES-GCM with a 16 octet ICV with 256-bit key length – Should

(2) 透過步驟(8)，IKE-AUTH 是由 IKEv2 的第一階段完整性演算法進行完整性保護。解密後的 IKE-AUTH 請求信令中含有 IKEv2 的第二階段完整性演算法需要符合以下標準。其演算法支援等級分為必須支援的 Shall 和建議支援的 Should，標記+代表演算法強度更強。

i AUTH_HMAC_SHA2_256_128 – Shall

ii AES_GCM with 16 octet ICV with 128-bit key length – Shall

iii AES_GCM with 16 octet ICV with 256-bit key length – Shall

iv AUTH_HMAC_SHA2_512_256 – Should

(3) 透過步驟(9)，封裝安全承載量資料封包是由 IKEv2 的第二階段完整性演算法進行完整性保護，將其解密後得到 F1AP 介面之用戶平面資料封包。

6.1.7.5 控制平面資料在 F1-U 介面的完整性保護

(a) 測試依據：

依據 3GPP TS 33.501 [11] 之第 5.3.9 小節與 O-RAN Security Test Specification[15]之第 6.5 小節，並參考 3GPP TS 33.210 [14] 之第 5.3.3 和 5.3.4 小節以及 3GPP TS 33.523 [9]之 7.2.2.1.4 小節。

(b) 測試目的：

驗證待測物 O-DU 的 F1-U 介面控制平面資料符合網際網路安全協定 (IPsec) 加密和認證達到完整性保護。

(c) 測試前提：

(1) 用戶設備及 O-CU 間可以進行接取層安全演算法設定。

(2) 與待測物的安全閘道器可以成功建立 IPsec 連線。

(3) 用戶設備採用 RuSIM 之模擬器時，待測物 O-DU 與 O-CU 間可以成功透過 IPsec 建立 F1AP 連線，且 RuSIM、待測物 O-DU、O-CU 及 5GC 間可以成

功建立 5G 連線。採用自動測試時，5GC 與 O-CU 需為 5gcuSIM 之模擬器，待測物 O-DU 與 5gcuSIM 間可以成功透過 IPsec 建立 F1AP 連線，RuSIM、待測物 O-DU、5gcuSIM 間可以成功建立 5G 連線。

(4) 待測物的安全閘道器(Security Gateway, SeGW)都可以支援 IKEv2，並可進行 IPsec 安全演算法設定。

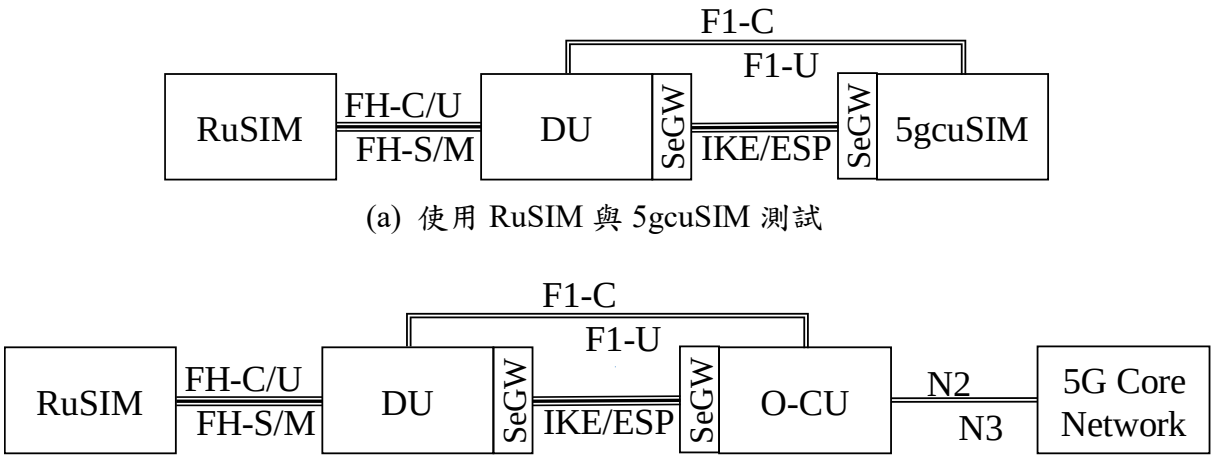
(5) 測試人員可採用分析工具或自動測試。

i. 採用工具分析時，需要擷取並解密 IPsec 介面封包，並分析 ISAKMP 與封裝安全承載內容。

ii. 採用自動測試時，需要透過 5gcuSIM 的 SeGW 直接解密 IPsec 介面封包，並分析 ISAKMP 與封裝安全承載內容。

(d) 測試佈局：

見圖 56。



(a) 使用 RuSIM 與 5gcuSIM 測試

(b) 使用 RuSIM 測試

圖 56 控制平面資料在 F1-C 介面機密性保護測試示意圖

(e) 測試步驟：

(1) 在用戶設備設定支援 NEA1、NEA2、NIA1、NIA2 機密和完整性安全演算法。

(2) 在 O-CU 端設定 NEA1、NIA1 機密和完整性安全演算法為最優先選擇。

(3) 採用工具分析時，開始擷取 IPsec 介面封包。

(4) 與待測物的安全閘道器建立 IPsec 連線。

(5) 採用工具分析時，確認待測物 O-DU 與 O-CU 或 5gcuSIM 間成功透過 IPsec 建立 F1AP 連線。採用自動測試時，確認與 5gcuSIM 成功連線。

(6) 確認用戶設備註冊上 5GC 或 5gcuSIM。

(7) 採用工具分析時，停止擷取 IPsec 介面封包。

(8) 採用工具分析時，透過 IPsec 介面封包，確認完成 IKE-SA-INIT 和 IKE-AUTH 程序並解密檢查其中之加密演算法。採用自動測試時，透過 5gcuSIM 端確認。

(9) 採用工具分析時，透過 IPsec 介面封包，確認使用封裝安全承載量進行資料傳輸並解密其封包。採用自動測試時，透過 5gcuSIM 端確認。

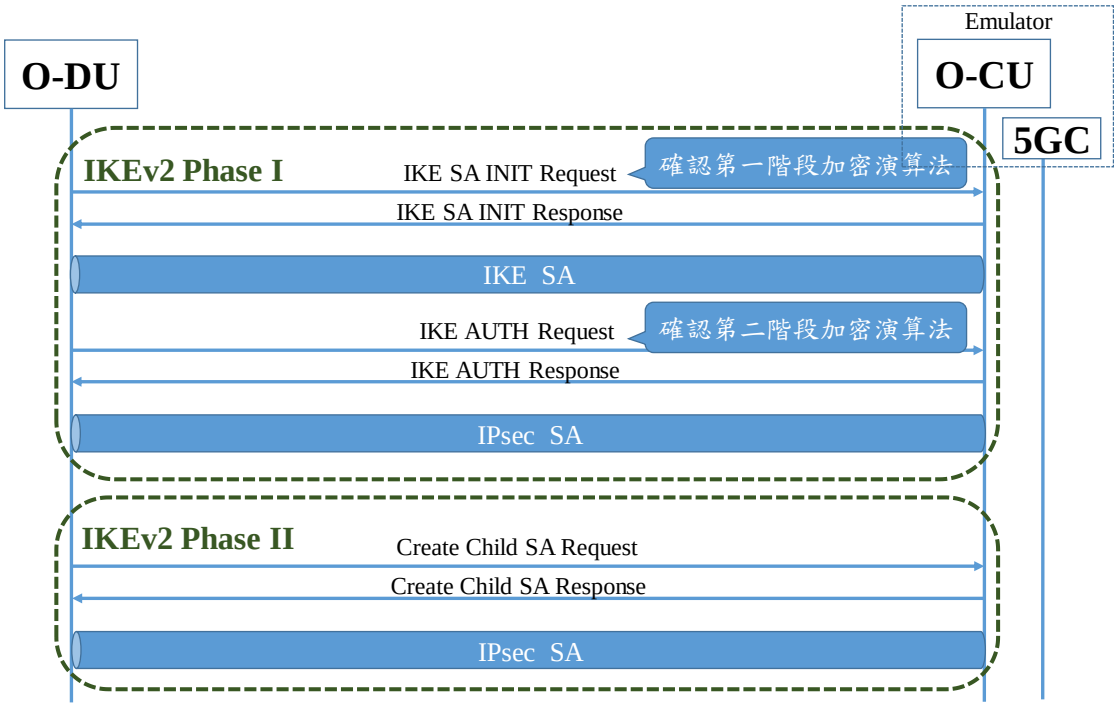


圖 57 控制平面資料在 F1-C 介面機密性保護測試流程圖

(f) 測試結果：

(1) 透過步驟(8)，IKE-SA-INIT 請求信令中含有 IKEv2 的第一階段完整性演算法需要符合以下標準。根據標準文件第 15 版和第 16 版，其演算法支援等級分為必須支援的 Shall 和建議支援的 Should。

第 15 版標準文件

i AUTH_HMAC_SHA1_96 - Shall

ii AUTH_HMAC_SHA2_256_128 - Shall

第 16 版標準文件

i AES-GCM with a 16 octet ICV with 128-bit key length – Shall

ii AES-GCM with a 16 octet ICV with 256-bit key length – Should

(2) 透過步驟(8)，IKE-AUTH 是由 IKEv2 的第一階段完整性演算法進行完整性保護。解密後的 IKE-AUTH 請求信令中含有 IKEv2 的第二階段完整性演算法需要符合以下標準。其演算法支援等級分為必須支援的 Shall 和建議支援的 Should，標記+代表演算法強度更強。

i AUTH_HMAC_SHA2_256_128 – Shall

ii AES_GCM with 16 octet ICV with 128-bit key length – Shall

iii AES_GCM with 16 octet ICV with 256-bit key length – Shall

iv AUTH_HMAC_SHA2_512_256 – Should

(3) 透過步驟(9)，封裝安全承載量資料封包是由 IKEv2 的第二階段完整性演算法進行完整性保護，將其解密後得到 F1-U 介面之用戶平面資料封包。

6.1.7.6 控制平面資料在 E2 介面的完整性保護

(a) 測試依據：

依據 O-RAN Security Test Specification [15]之 6.5 和 13.2 小節，並參考 O-RAN Security Protocols Specification [19]之第 2.2 小節與 3GPP TS 33.210 [14] 之第 5.3.3 和 5.3.4 小節。

(b) 測試目的：

驗證待測物 O-DU 的 E2 介面控制平面資料符合網際網路安全協定 (IPsec) 加密和認證達到完整性保護。

(c) 測試前提：

(1) 用戶設備及 O-CU 間可以進行接取層安全演算法設定。

(2) 與待測物的安全閘道器間可以成功建立 IPsec 連線。

(3) 用戶設備可以採用 RuSIM，待測物 O-DU 與 Near-RT RIC 間可以成功透過 IPsec 建立 E2AP 連線。採用自動測試時，Near-RT RIC 需為 RicSIM 之模擬器，待測物 O-DU 與 RicSIM 間可以成功透過 IPsec 建立 E2AP 連線，RuSIM、待測物 O-DU、O-CU 與 5GC 間可以成功建立 5G 連線。

(4) 待測物的安全閘道器(Security Gateway, SeGW)可以支援 IKEv2，並可進行 IPsec 安全演算法設定。

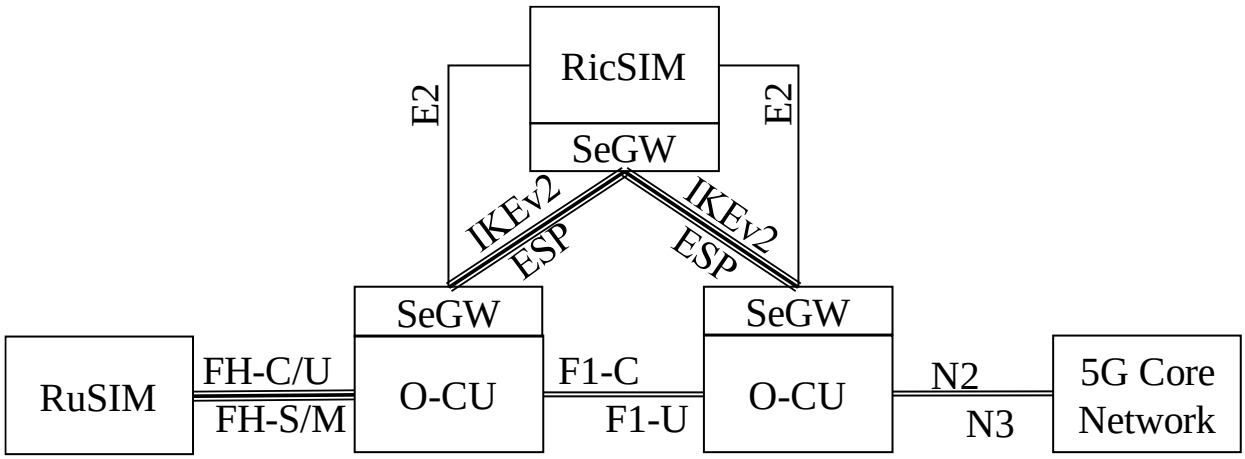
(5) 測試人員可採用分析工具或自動測試。

i. 採用工具分析時，需要擷取並解密 IPsec 介面封包，並分析 ISAKMP 與封裝安全承載內容。

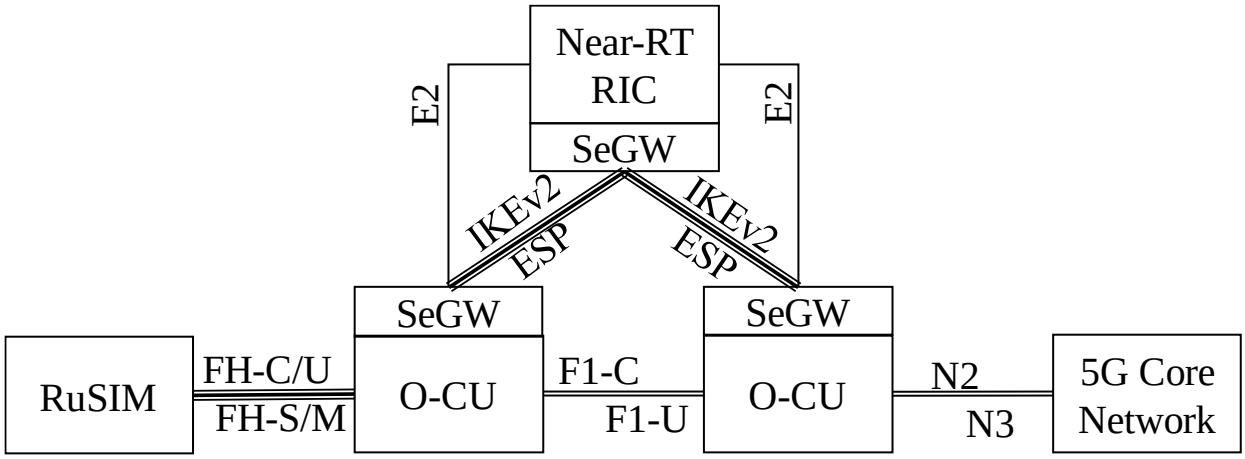
ii. 採用自動測試時，需要透過 RicSIM 的 SeGW 直接解密 IPsec 介面封包，並分析 ISAKMP 與封裝安全承載內容。

(d) 測試佈局：

見圖 58。



(a) 使用 RuSIM 與 RicSIM 測試



(b) 使用 RuSIM 測試

圖 58 控制平面資料在 E2 介面機密性保護測試示意圖

(e) 測試步驟：

(1) 在用戶設備設定支援 NEA1、NEA2、NIA1、NIA2 機密和完整性安全演算法。

(2) 在 O-CU 端設定 NEA1、NIA1 機密和完整性安全演算法為最優先選擇。

(3) 採用工具分析時，開始擷取 IPsec 介面封包。

(4) 待測物的安全閘道器建立 IPsec 連線。

(5) O-CU 與 Near-RT RIC 間可以成功透過 IPsec 建立 E2AP 連線。

(6) 確認待測物 O-DU 與 Near-RT RIC 間可以成功透過 IPsec 建立 E2AP 連線，且待測物 O-DU 與 O-CU 建立 F1AP 連線。採用自動測試時，Near-RT RIC 需為 RicSIM。

(7) 確認 O-CU 與 5GC 建立 NGAP 連線，且用戶設備註冊上 5GC。

(8) 採用工具分析時，停止擷取 IPsec 介面封包。

(9) 採用工具分析時，透過 IPsec 介面封包，確認完成 IKE-SA-INIT 和 IKE-AUTH 程序並解密檢查其中之加密演算法。採用自動測試時，透過 RicSIM 端確認。

(10) 採用工具分析時，透過 IPsec 介面封包，確認使用封裝安全承載量進行資料傳輸並解密其封包。採用自動測試時，透過 RicSIM 端確認。

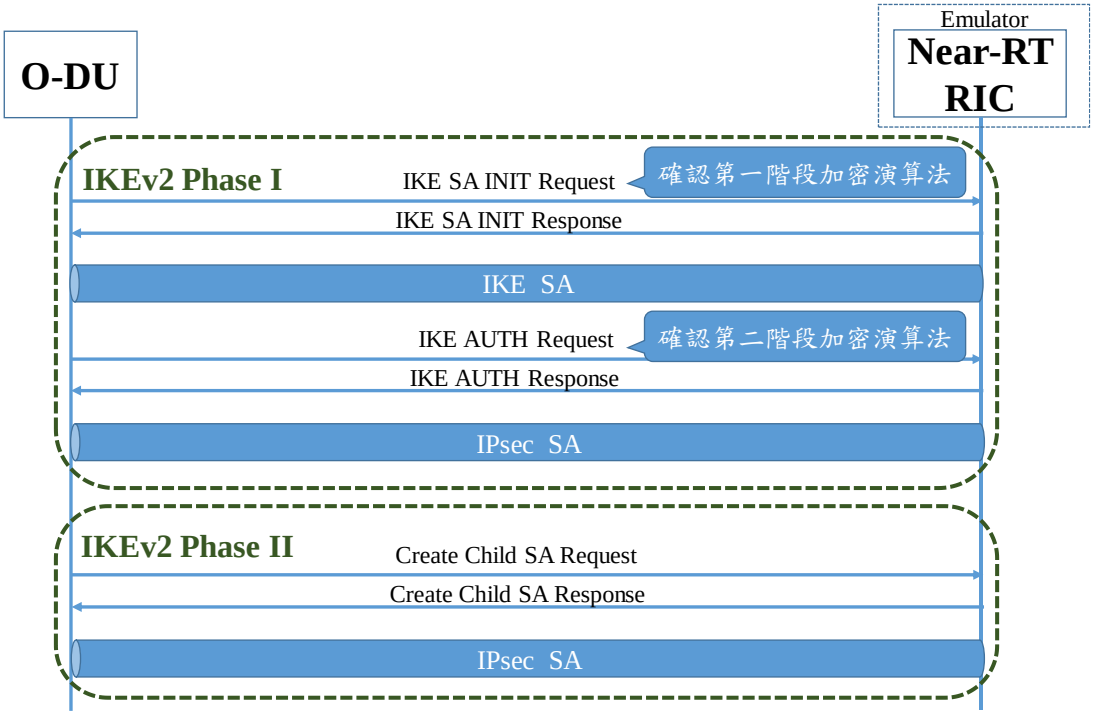


圖 59 控制平面資料在 E2 介面機密性保護測試流程圖

(f) 測試結果：

(1) 透過步驟(8)，IKE-SA-INIT 請求信令中含有 IKEv2 的第一階段完整性演算法需要符合以下標準。根據標準文件第 15 版和第 16 版，其演算法支援等級分為必須支援的 Shall 和建議支援的 Should。

第 15 版標準文件

i AUTH_HMAC_SHA1_96 - Shall

ii AUTH_HMAC_SHA2_256_128 - Shall

第 16 版標準文件

i AES-GCM with a 16 octet ICV with 128-bit key length – Shall

ii AES-GCM with a 16 octet ICV with 256-bit key length – Should

(2) 透過步驟(8)，IKE-AUTH 是由 IKEv2 的第一階段完整性演算法進行完整性保護。解密後的 IKE-AUTH 請求信令中含有 IKEv2 的第二階段完整性演算法需要符合以下標準。其演算法支援等級分為必須支援的 Shall 和建議支援的 Should，標記+代表演算法強度更強。

i AUTH_HMAC_SHA2_256_128 – Shall

ii AES_GCM with 16 octet ICV with 128-bit key length – Shall

iii AES_GCM with 16 octet ICV with 256-bit key length – Shall

iv AUTH_HMAC_SHA2_512_256 – Should

(3) 透過步驟(9)，封裝安全承載量資料封包是由 IKEv2 的第二階段完整性演算法進行完整性保護，將其解密後得到 E2 介面之用戶平面資料封包。

6.1.8 O-DU 介面功能安全性檢測

6.1.8.1 F1-C 介面的模糊測試 (非必測項目)

(a) 測試依據：

參考 O-RAN Security Test Specification[15]之第 7.4 小節與 3GPP TS 33.117 [2]之第 4.4.4 小節。

(b) 測試目的：

驗證待測物 O-DU 的 F1-C 介面能夠適當處裡非預期的 F1AP 封包。

(c) 測試前提：

(1) RuSIM 可成功與待測物 O-DU 以及 O-CU 模糊測試器建立 5G 連線。

(2) 測試人員可採用分析工具或自動測試。

i. 採用工具分析時，擷取 F1AP 封包並分析其封包內容。

ii. 採用自動測試時，需要透過 O-CU 模糊測試器分析 F1AP 封包內容。

(d) 測試佈局：

見圖 60。

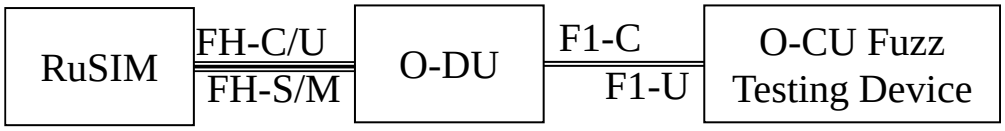


圖 60 F1-C 介面的模糊測試示意圖

(e) 測試步驟：

(1) 採用工具分析時，開始擷取 F1-C 介面封包。

(2) 待測物 O-DU 可成功 O-CU 模糊測試器建立 F1AP 連線。

(3) O-CU 模糊測試器對待測物 O-DU 發送非預期的 F1AP 封包。

(4) 採用工具分析時，停止擷取 F1AP 封包。

(5) 採用工具分析時，透過 F1AP 封包，確認待測物 O-DU 是否捨棄非預期的 F1AP 封包亦或回覆 F1AP 封包錯誤。採用自動測試時，由 O-CU 模糊測試器確認。

(6) 應用協定介面封包，待測物 O-DU 重新與 O-CU 模糊測試器建立 F1AP 連線。

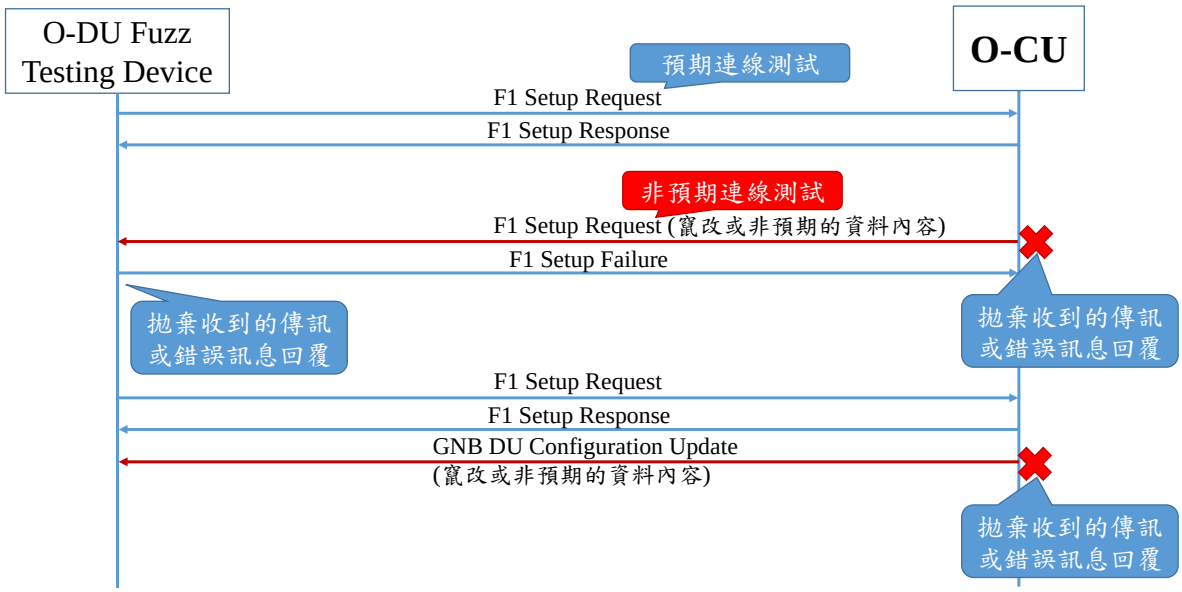


圖 61 F1-C 介面的模糊測試流程圖

(f) 測試結果：

(1) 根據步驟(5)和(6)，O-DU 捨棄非預期的 F1AP 封包或回覆 F1AP 封包錯誤，並持續與建立 F1AP 連線。

6.1.8.2 開放前傳介面 C-Plane 模糊測試(非必測項目)

(a) 測試依據:

依據 O-RAN TIFG E2E-Test [17]之第 7.2.5 小節。

(b) 測試目的:

驗證待測物 O-DU 的 Open FH 介面 C-Plane 遭受非預期訊號攻擊時，O-DU 的性能不會受到影響。

(c) 測試前提:

(1) 對待測物 O-DU 實施 O-RAN TIFG E2E-Test [17]之第 5.6 小節與第 6.1 小節的測試項目。

(2) UE、O-RU、待測物 O-DU、O-CU 及 5GC 端可成功建立 5G 連線。

(3) O-RU 模糊測試器能夠連接到待測物 O-DU 的 Open FH 介面 C-Plane。

(d) 測試佈局：

見圖 62。

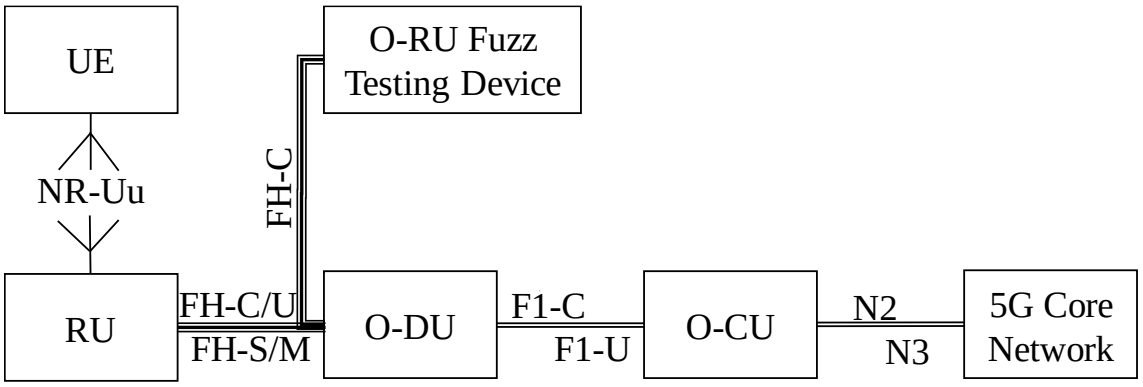


圖 62 Open FH 介面 C-Plane 的模糊測試示意圖

(e) 測試步驟:

(1) O-RU 模糊測試器對於待測物 O-DU 的 Open FH 介面 C-Plane 產生透過乙太網路發送之演進版通用公共無線電介面控制信令 (eCPRI real-time ctrl data message) 之非預期訊號攻擊封包。

(2) O-RU 模糊測試器的來源媒體存取控制位址 (MAC address) 須為 O-RU 的位址，但是須篡改 C-Plane 的非預期訊號攻擊封包內容。

(3) O-RU 模糊測試器產生 250,000 次的非預期訊號攻擊流量。

(4) 對待測物 O-DU 實施 O-RAN TIFG E2E-Test [17]之第 5.6 小節與第 6.1 小節的測試項目。

(f) 測試結果:

(1) 根據步驟(4)，確認 O-DU 的性能不會受到影響。

6.1.8.3 開放前傳介面 S-Plane 模糊測試(非必測項目)

(a) 測試依據:

依據 O-RAN TIFG E2E-Test [20]之第 7.2.4 小節。

(b) 測試目的:

驗證待測物 O-DU 的 Open FH 介面 S-Plane 遭受非預期訊號攻擊時，O-DU 的性能不會受到影響。

(c) 測試前提:

(1) 待測物 O-DU 通過 O-RAN TIFG E2E-Test [17]之第 5.6 小節與第 6.1 小節的測試項目。

(2) UE、O-RU、待測物 O-DU、O-CU 及 5GC 端可成功建立 5G 連線。

(3) O-RU 模糊測試器能夠連接到待測物 O-DU 的 Open FH 介面 S-Plane。

(d) 測試佈局：

見圖 63。

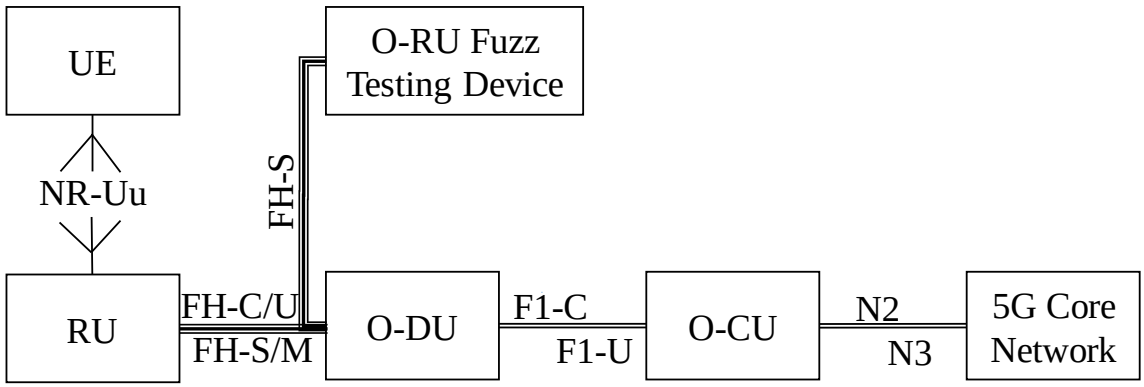


圖 63 Open FH 介面 S-Plane 的模糊測試示意圖

(e) 測試步驟:

(1) O-RU 模糊測試器對於待測物 O-DU 的 Open FH 介面 S-Plane 產生常態性乙太網路訊框(generic Ethernet frames)及高精確時間協定 (PTP) announce/sync 信令之非預期訊號攻擊封包。

(2) O-RU 模糊測試器的來源媒體存取控制位址 (MAC address) 須為 RuSIM 的位址，但是須篡改 S-Plane 的非預期訊號攻擊封包內容。

(3) O-RU 模糊測試器產生 250,000 次的非預期訊號攻擊流量。

(4) 對待測物 O-DU 實施 O-RAN TIFG E2E-Test [17]之第 5.6 小節與第 6.1 小節的測試項目。

(f) 測試結果:

(1) 根據步驟(4)，確認 O-DU 的性能不會受到影響。

6.1.8.4 開放前傳介面 C-Plane 阻斷服務測試(非必測項目)

(a) 測試依據:

依據 O-RAN TIFG E2E-Test [20]之第 7.2.2 小節。

(b) 測試目的:

驗證待測物 O-DU 的 Open FH 介面 C-Plane 遭受阻斷服務攻擊時，O-DU 的性能不會受到影響。

(c) 測試前提:

(1) 對待測物 O-DU 實施 O-RAN TIFG E2E-Test [17]之第 5.6 小節與第 6.1 小節的測試項目。

(2) UE、O-RU、待測物 O-DU、O-CU 及 5GC 端可成功建立 5G 連線。

(3) O-RU 阻斷服務攻擊模擬器能夠連接到待測物 O-DU 的 Open FH 介面 S-Plane。

(d) 測試佈局：

見圖 64。

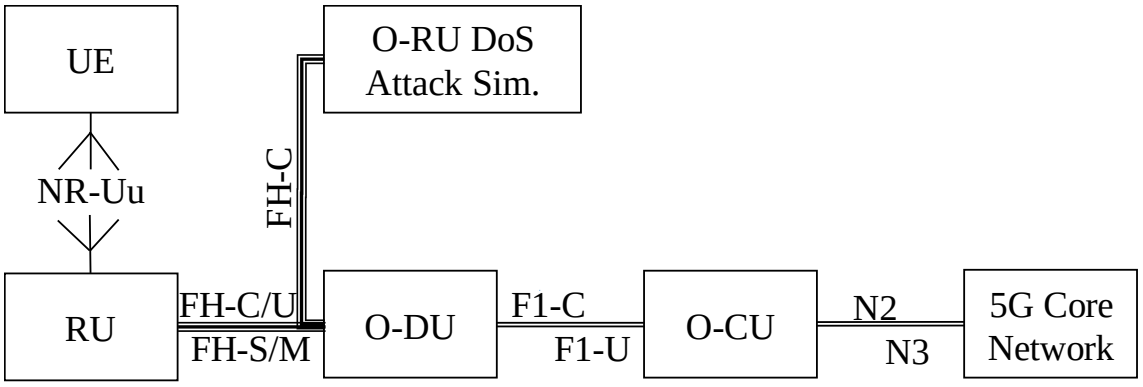


圖 64 Open FH 介面 C-Plane 阻斷服務測試示意圖

(e) 測試步驟:

(1) O-RU 阻斷服務攻擊模擬器對於待測物 O-DU 的 Open FH 介面 S-Plane 產生常態性乙太網路訊框(generic Ethernet frames)及高精確時間協定 (PTP) announce/sync 信令之阻斷服務攻擊封包。

(2) O-RU 阻斷服務攻擊模擬器的攻擊流量為 10Mbps、100Mbps 與 1Gbps。

(3) O-RU 阻斷服務攻擊模擬器產生之攻擊封包的媒體存取控制位址(MAC address) 須為篡改的 PTPGM 位址、隨機位址和廣播位址。

(4) 對待測物 O-DU 實施 O-RAN TIFG E2E-Test [17]之第 5.6 小節與第 6.1 小節的測試項目。

(f) 測試結果:

(1) 根據步驟(4)，確認 O-DU 的性能不會受到影響。

6.1.8.5 開放前傳介面 S-Plane 阻斷服務測試(非必測項目)

(a) 測試依據:

依據 O-RAN TIFG E2E-Test [20]之第 7.2.1 小節。

(b) 測試目的:

驗證待測物 O-DU 的開放前傳介面 S-Plane 遭受阻斷服攻擊時，O-DU 的性能不會受到影響。

(c) 測試前提:

(1) 對待測物 O-DU 實施 O-RAN TIFG E2E-Test [17]之第 5.6 小節與第 6.1 小節的測試項目。

(2) UE、O-RU、待測物 O-DU、O-CU 及 5GC 端可成功建立 5G 連線。

(3) O-RU 阻斷服務攻擊模擬器能夠連接到待測物 O-DU 的開放前傳介面 S-Plane。

(d) 測試佈局：

見圖 65。

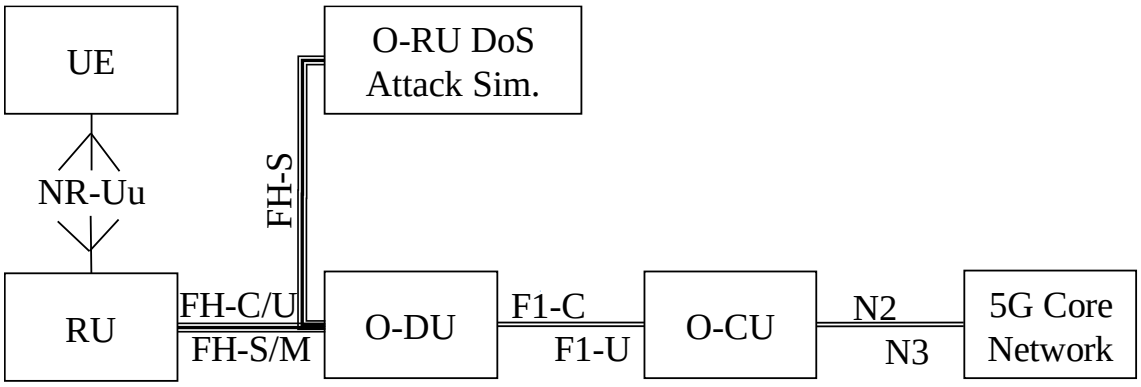


圖 65 開放前傳介面 S-Plane 阻斷服務測試示意圖

(e) 測試步驟:

(1) O-RU 阻斷服務攻擊模擬器對於待測物 O-DU 的開放前傳介面 S-Plane 產生常態性乙太網路訊框(generic Ethernet frames)及高精確時間協定 (PTP) announce/sync 信令之阻斷服攻擊封包。

(2) O-RU 阻斷服務攻擊模擬器的攻擊流量為 10Mbps、100Mbps 與 1Gbps。

(3) O-RU 阻斷服務攻擊模擬器產生之攻擊封包的媒體存取控制位址(MAC address) 須為篡改的 PTPGM 位址、隨機位址和廣播位址。

(4) 對待測物 O-DU 實施 O-RAN TIFG E2E-Test [17]之第 5.6 小節與第 6.1 小節的測試項目。

(f) 測試結果:

(1) 根據步驟(4)，確認 O-DU 的性能不會受到影響。

6.1.9 O-DU 與 O-RU 介面功能安全性檢測

6.1.9.1 安全外殼協定(SSH)的安全測試

(a) 測試依據:

依據 O-RAN Security Test Specification[15]之第 6.2 小節，並參考 O-RAN Security Protocols Specification[19]之第 2.1 小節。

(b) 測試目的:

驗證待測物 O-RU 或待測物 O-DU 之 Open FH 介面 M-plane 的 SSH 協定受到安全保護。

(c) 測試前提:

(1) 待測物 O-RU 或待測物 O-DU 可以支援第二版(v2)的 SSH 安全協定。

(2) SSH 協定測試工具可以透過 Open FH 介面 M-plane 與待測物 O-RU 或待測物 O-DU 建立 SSH 連線。

(3) SSH 協定測試工具可以模擬 SSH 協定用戶端與 SSH 協定伺服器。

(4) 測試人員可採用分析工具或自動測試。

i. 採用工具分析時，需要擷取 Open FH 介面 M-plane 封包，並分析 SSH 協定內容。

ii. 採用自動測試時，需要透過 SSH 協定測試工具直接解密 Open FH 介面 M-plane 封包，並分析封包內容。

(d) 測試佈局：

見圖 66。

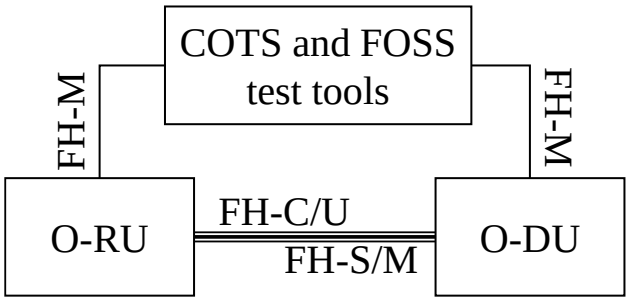


圖 66 安全外殼協定(SSH)的安全測試示意圖

(e) 測試步驟:

(1) 待測物 O-RU 或待測物 O-DU 設定使用第二版(v2)的 SSH 安全協定。

(2) 採用工具分析時，開始擷取 Open FH 介面 M-plane 封包。

(3) SSH 協定測試工具設定模擬 SSH 協定用戶端(或 SSH 協定伺服器)。

i. 當 SSH 協定測試工具設定模擬 SSH 協定用戶端時，SSH 協定測試工具透過 Open FH 介面 M-plane 與待測物建立 SSH 連線。

ii. 當 SSH 協定測試工具設定模擬 SSH 協定伺服器時，待測物透過 Open FH 介面 M-plane 與 SSH 協定測試工具建立 SSH 連線。

(4) 採用工具分析時，停止擷取 Open FH 介面 M-plane 封包。

(5) 採用工具分析時，分析 Open FH 介面 M-plane 封包，確認使用第二版(v2)的 SSH 安全協定。採用自動測試時，由 SSH 協定測試工具分析。

(6) 採用工具分析時，分析 Open FH 介面 M-plane 封包，確認 SSH 安全協定使用之主機密鑰演算法(Host key algorithms)、加解密資料的對稱演算法(Symmetric algorithms for encrypting data)與金鑰交換演算法(Key exchange algorithms)及訊息鑑別碼 (Message Authentication Code, MACs)內容。採用自動測試時，由 SSH 協定測試工具確認。

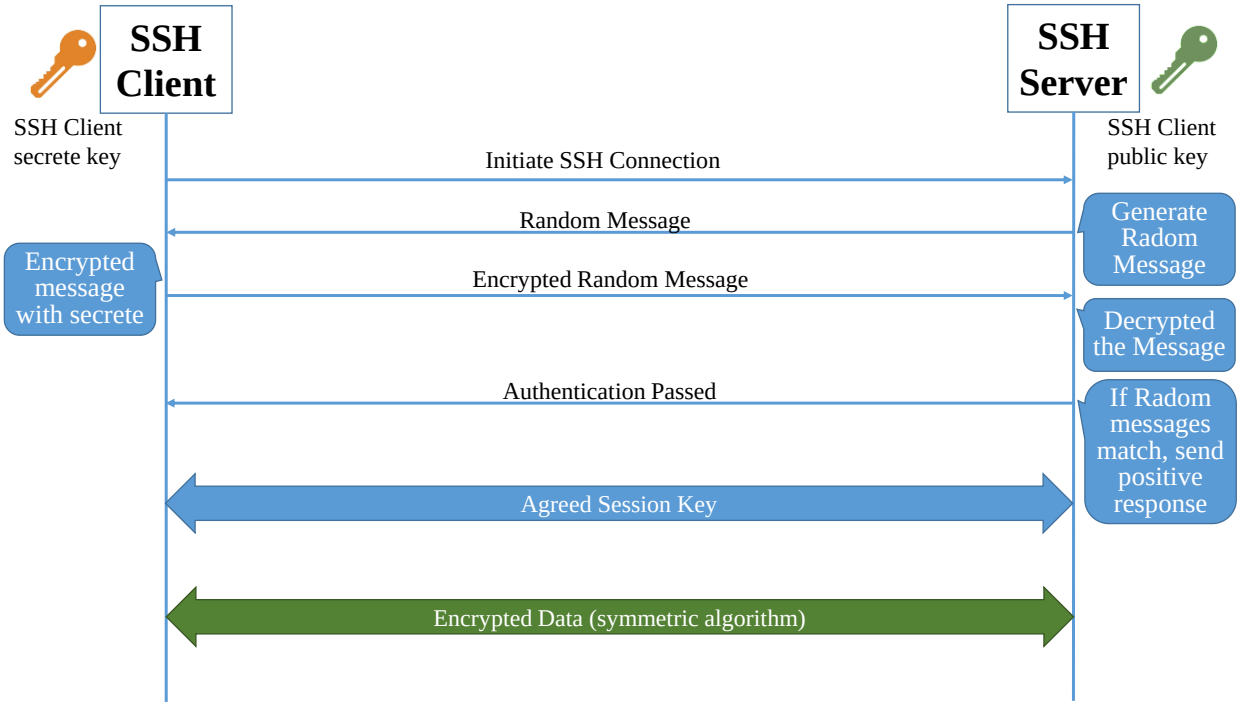


圖 67 安全外殼協定(SSH)的安全測試流程圖

(f) 測試結果:

(1) 透過步驟(6)，確認待測物 O-RU 或待測物 O-DU 的 Open FH 介面 M-plane 使用第二版(v2)的 SSH 安全協定。

(2) 透過步驟(6)，確認待測物 O-RU 或待測物 O-DU 的 Open FH 介面 M-plane 的 SSH 安全協定需要符合以下標準。

[1] 主機密鑰演算法(Host key algorithms)需要使用以下標準。

i ecdsa-sha2-nistp256

ii ecdsa-sha2-nistp384

iii ecdsa-sha2-nistp521

iv ssh-ed25519 (support began in OpenSSH 6.5)

v ssh-ed448

主機密鑰演算法(Host key algorithms)不能使用以下標準。

i ssh-rsa

ii ssh-dss

[2] 加解密資料的對稱演算法(Symmetric algorithms for encrypting data) 需要使用以下標準。

i aes256-gcm

ii aes128-gcm

iii aes256-ctr

iv aes192-ctr

v aes128-ctr

[3] 金鑰交換演算法(Key exchange algorithms, KexAlgorithms) 需要使用以下標準。

i ecdh-sha2-nistp521

ii ecdh-sha2-nistp384

iii ecdh-sha2-nistp256

iv diffie-hellman-group-exchange-sha256

v curve25519-sha256

金鑰交換演算法(Key exchange algorithms, KexAlgorithms) 不能使用以下標準。

i diffie-hellman-group1-sha1

[4] 訊息鑑別碼 (Message Authentication Code, MACs)需要使用以下標準。

i hmac-sha2-512-etm

ii hmac-sha2-512

iii hmac-sha2-256-etm

iv hmac-sha2-256

v umac-128

訊息鑑別碼 (Message Authentication Code, MACs)不能使用以下標準。

i hmac-sha1

6.1.9.2 驗證者驗證

(a) 測試依據:

依據 O-RAN Security Test Specification[15]之第 6.4 小節。

(b) 測試目的:

驗證 O-RU 及 O-DU 間的 Open FH 介面受到安全保護。

(c) 測試前提:

(1) 安全閘道器(Security Gateway)可以支援遠程鑑別撥入用戶服務(Remote Authentication Dial In User Service, RADIUS)，並可進行 eap.conf 等*.conf 之安全演算法設定。

(2) 用戶設備可以採用 UE 或 RuSIM 之模擬器。

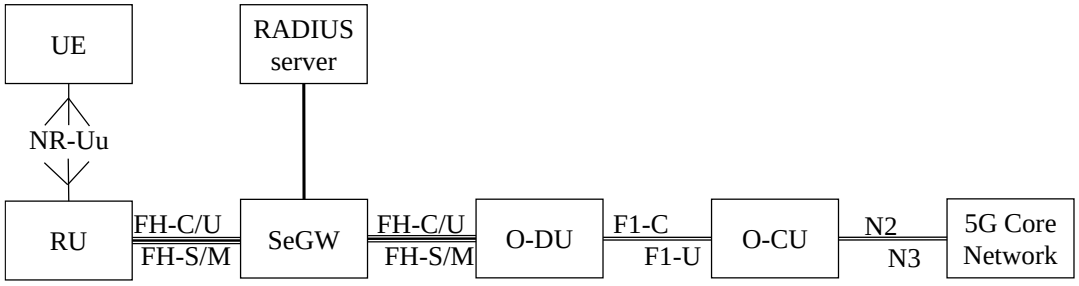
i. 當用戶設備使用 UE 時，O-RU 與 O-DU 間可以成功透過安全閘道器(Security Gateway)建立 Open FH 介面連線，且 UE、O-RU、O-DU、O-CU 及 5GC 間可以成功建立 5G 連線。

ii. 當用戶設備使用 RuSIM 時，RuSIM 與 O-DU 間可以成功透過安全閘道器(Security Gateway)建立 Open FH 介面連線，且 RuSIM、O-DU、O-CU 及 5GC 間可以成功建立 5G 連線。

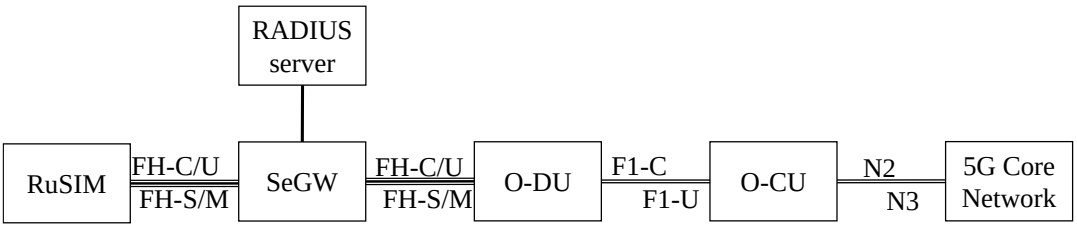
(3) 測試人員可擷取並解密安全閘道器(Security Gateway)封包，並分析封包內容。

(d) 測試佈局：

見圖 68。



(a) 使用 UE 測試



(b) 使用 RuSIM 測試

圖 68 驗證者驗證的安全測試示意圖

(e) 測試步驟:

(1) 於驗證者(Authenticator)端，針對透過區域網路(Extensible Authentication Protocol over LAN, EAPoL)設定正確的識別符-認證區別名(Certificate Distinguished 可延伸鑑別協定(Extensible Authentication ProtocolName, Certificate DN)與正確的用戶端認證(Client Certificate)。

(2) 開始擷取安全閘道器(Security Gateway)封包。

(3) 用戶設備可以採用 UE 或 RuSIM 之模擬器。

i. 當用戶設備使用 UE 時，確認 O-RU 與 O-DU 可以成功透過驗證者(Supplicant)進行遠程鑑別撥入用戶服務(RADIUS)認證。O-RU 與 O-DU 透過安全閘道器(Security Gateway)建立 Open FH 介面連線。

ii. 當用戶設備使用 RuSIM 時，確認 RuSIM 模擬器與 O-DU 可以成功透過驗證者(Supplicant)進行遠程鑑別撥入用戶服務(RADIUS)認證。RuSIM 模擬器與 O-DU 透過安全閘道器(Security Gateway)建立 Open FH 介面連線。

(4) 確認 DU 與 O-CU 建立 F1AP 連線

(5) 確認 O-CU 與 5GC 建立 NGAP 連線，且用戶設備註冊上 5GC。

(6) 停止擷取安全閘道器(Security Gateway)介面封包。

(7) 確認與遠程鑑別撥入用戶服務(RADIUS)伺服器的認證狀態。

(8) 於驗證者(Authenticator)端，針對透過區域網路可延伸鑑別協定(EAPoL)分別設定如下，並重複(2)~(7)測試步驟

i. 正確的識別符-認證區別名(Certificate DN)與錯誤的用戶端認證(Client Certificate)設定。

ii. 錯誤的識別符-認證區別名(Certificate DN)。

iii. 使用非傳送層安全之可延伸鑑別協定(Extensible Authentication Protocol non-Transport Layer Security, EAP non-TLS)

(f) 測試結果:

(1) 透過步驟(7)，透過區域網路可延伸鑑別協定(EAPoL)設定正確的識別符-認證區別名(Certificate DN)與正確的用戶端認證(Client Certificate)時，與遠程鑑別撥入用戶服務(RADIUS)伺服器將會成功完成認證。

(2) 當透過區域網路可延伸鑑別協定(EAPoL)設定正確的識別符-認證區別名(Certificate DN)與錯誤的用戶端認證(Client Certificate)設定、設定錯誤的識別符-認證區別名(Certificate DN)或使用非傳送層安全之可延伸鑑別協定(EAP non-TLS) 時，與遠程鑑別撥入用戶服務(RADIUS)伺服器的認證結果會失敗。

6.1.9.3 申請者驗證

(a) 測試依據:

依據 O-RAN Security Test Specification[15]之第 6.4 小節。

(b) 測試目的:

驗證 O-RU 及 O-DU 間的 Open FH 介面受到安全保護。

(c) 測試前提:

(1) 安全閘道器(Security Gateway)可以支援遠程鑑別撥入用戶服務(Remote Authentication Dial In User Service, RADIUS)，並可進行 eap.conf 等*.conf 之安全演算法設定。

(2) 用戶設備可以採用 UE 或 RuSIM 之模擬器。

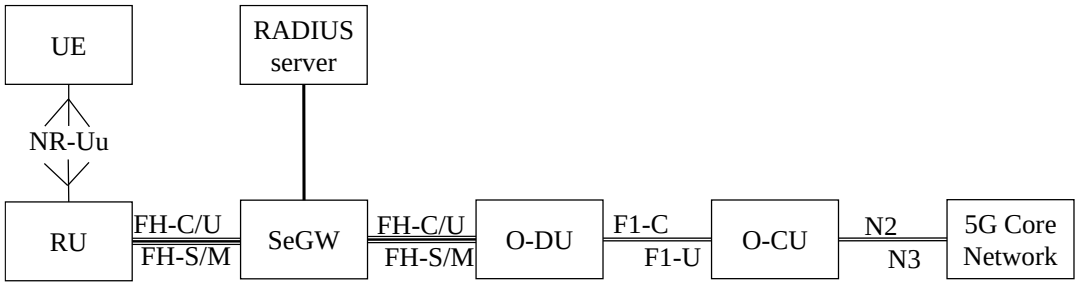
i. 當用戶設備使用 UE 時，確認 O-RU 與 O-DU 可以成功透過驗證者(Supplicant)進行遠程鑑別撥入用戶服務(RADIUS)認證。O-RU 與 O-DU 透過安全閘道器(Security Gateway)建立 Open FH 介面連線。

ii. 當用戶設備使用 RuSIM 時，確認 RuSIM 模擬器與 O-DU 可以成功透過驗證者(Supplicant)進行遠程鑑別撥入用戶服務(RADIUS)認證。RuSIM 模擬器與 O-DU 透過安全閘道器(Security Gateway)建立 Open FH 介面連線。

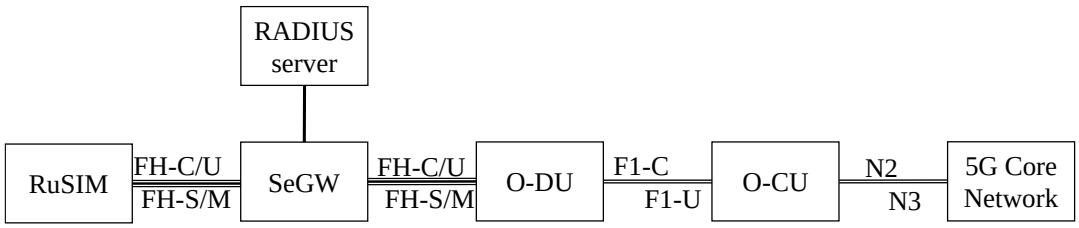
(3) 測試人員可擷取並解密安全閘道器(Security Gateway)封包，並分析封包內容。

(d) 測試佈局：

見圖 69。



(a) 使用 UE 測試



(b) 使用 RuSIM 測試

圖 69 申請者驗證的安全測試示意圖

(e) 測試步驟:

(1) 於申請者(Supplicant)端，針對透過區域網路(Extensible Authentication Protocol over LAN, EAPoL)設定正確的識別符-認證區別名(Certificate

Distinguished 可延伸鑑別協定(Extensible Authentication ProtocolName, Certificate DN)與正確的用戶端認證(Client Certificate)。

(2) 開始擷取安全閘道器(Security Gateway)封包。

(3) 用戶設備可以採用 UE 或 RuSIM 之模擬器。

i. 當用戶設備使用 UE 時，確認 O-RU 與 O-DU 可以成功透過驗證者(Supplicant)進行遠程鑑別撥入用戶服務(RADIUS)認證。O-RU 與 O-DU 透過安全閘道器(Security Gateway)建立 Open FH 介面連線。

ii. 當用戶設備使用 RuSIM 時，確認 RuSIM 模擬器與 O-DU 可以成功透過驗證者(Supplicant)進行遠程鑑別撥入用戶服務(RADIUS)認證。RuSIM 模擬器與 O-DU 透過安全閘道器(Security Gateway)建立 Open FH 介面連線。

(4) 確認 DU 與 O-CU 建立 F1AP 連線

(5) 確認 O-CU 與 5GC 建立 NGAP 連線，且用戶設備註冊上 5GC。

(6) 停止擷取安全閘道器(Security Gateway)介面封包。

(7) 確認與遠程鑑別撥入用戶服務(RADIUS)伺服器的認證狀態。

(8) 於申請者(Supplicant)端，針對透過區域網路可延伸鑑別協定(EAPoL)分別設定如下，並重複(2)~(7)測試步驟

i. 正確的識別符-認證區別名(Certificate DN)與錯誤的用戶端認證(Client Certificate)設定。

ii. 錯誤的識別符-認證區別名(Certificate DN)。

iii. 使用非傳送層安全之可延伸鑑別協定(Extensible Authentication Protocol non-Transport Layer Security, EAP non-TLS)

(f) 測試結果:

(1) 透過步驟(7)，透過區域網路可延伸鑑別協定(EAPoL)設定正確的識別符-認證區別名(Certificate DN)與正確的用戶端認證(Client Certificate)時，與遠程鑑別撥入用戶服務(RADIUS)伺服器將會成功完成認證。

(2) 當透過區域網路可延伸鑑別協定(EAPoL)設定正確的識別符-認證區別名(Certificate DN)與錯誤的用戶端認證(Client Certificate)設定、設定錯誤的識別符-認證區別名(Certificate DN)或使用非傳送層安全之可延伸鑑別協定(EAP non-TLS) 時，與遠程鑑別撥入用戶服務(RADIUS)伺服器的認證結果會失敗。

6.1.10 RIC 安全通道檢測

6.1.10.1 資料包傳送層安全協定(DTLS)的安全測試(使用 IPsec 時無須測試)

(a) 測試依據:

依據 O-RAN Security Test Specification[15]之第 6.4 小節，並參考 O-RAN Security Protocols Specification[19]之第 2.4 小節。

(b) 測試目的:

驗證 Near-RT RIC 與 O-CU 及 O-DU 間的 E2 介面、F1-C 介面與 F1-U 介面受到安全保護。

(c) 測試前提:

(1) 待測物可以支援 DTLS v1.2 的安全協定。

(2) 測試人員可採用分析工具或自動測試

i. 採用工具分析時，擷取 E2 介面、F1-C 介面與 F1-U 介面封包，並分析 DTLS 協定內容。

ii. 採用自動測試時，需要透過 DTLS 協定測試工具直接解密 E2 介面、F1-C 介面與 F1-U 封包，並分析封包內容。

(d) 測試佈局：

見圖 6。

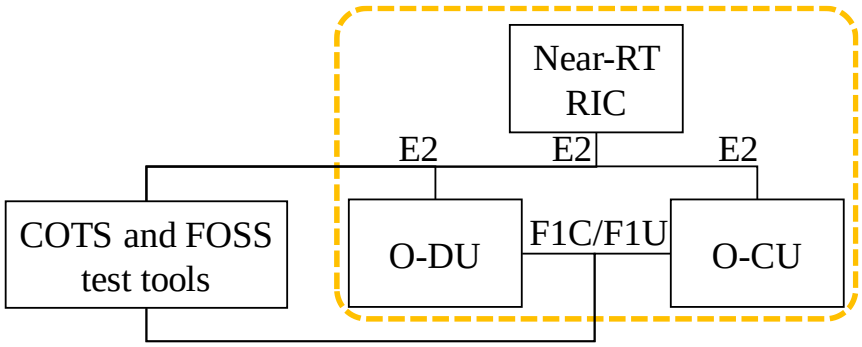


圖 70 資料包傳送層安全協定(DTLS)的安全測試示意圖

(e) 測試步驟:

(1) 待測物設定使用 DTLS v1.2 的安全協定。

(2) 採用工具分析時，開始擷取 E2 介面、F1-C 介面與 F1-U 介面封包。

(3) 確認 O-DU 與 O-CU 建立 F1AP 連線，O-DU 和 O-CU 分別與 Near-RT RIC 建立 E2AP 連線，O-CU 與 5GC 建立 NGAP 連線，且用戶設備註冊上 5GC 並收送數據資料。

(4) 採用工具分析時，

(5) 採用工具分析時，分析 E2 介面、F1-C 介面與 F1-U 介面封包，確認使用 DTLS v1.2 的安全協定。採用自動測試時，由 DTLS 協定測試工具確認。

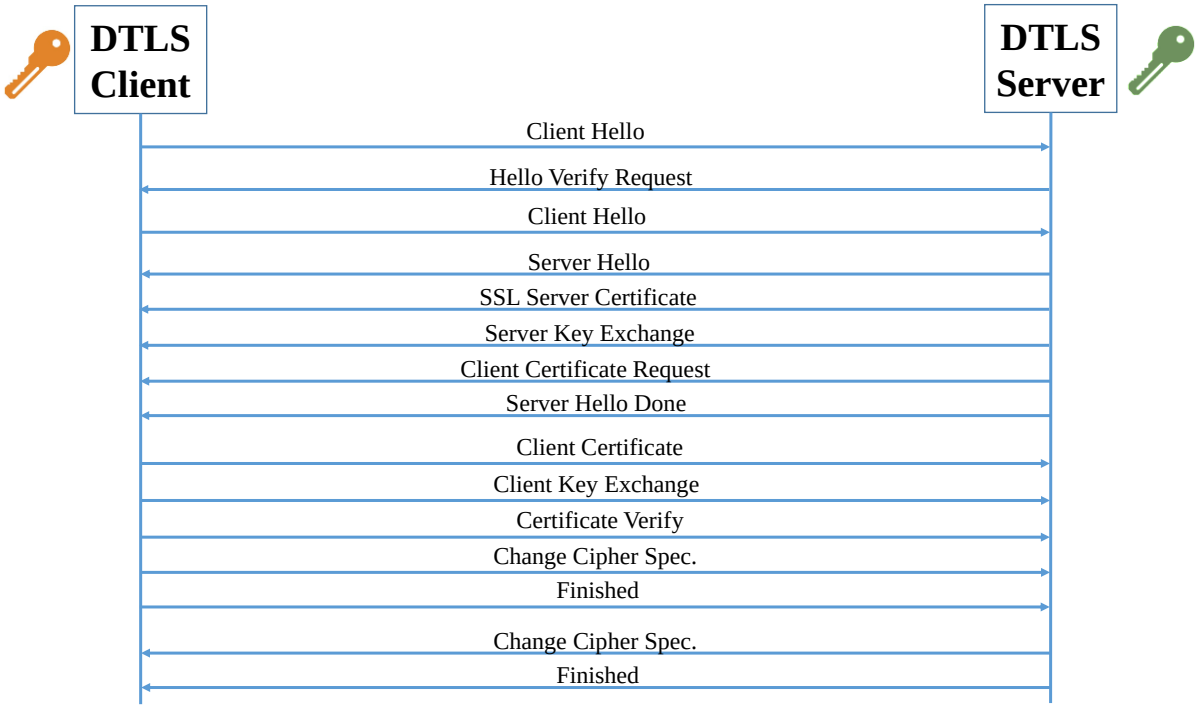


圖 71 資料包傳送層安全協定(DTLS)的安全測試流程圖

(f) 測試結果:

(1) 透過步驟(5)，待測物的 E2 介面、F1-C 介面與 F1-U 介面使用 TLS v1.2 的安全協定。

(2) 透過步驟(5)，確認待測物的 DTLS 1.2 中間密碼(Intermediate Ciphers for TLS 1.2)符合以下標準。

I. 加密套件 (TLS 1.2): (Only cipher suites with AEAD (e.g. GCM) and PFS (e.g. ECDHE, DHE) shall be supported)

i. TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

ii. TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

iii. TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

iv. TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

v. TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256

vi. TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256

vii. TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

viii. TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

ix. TLS_DHE_PSK_WITH_AES_128_GCM_SHA256

x. TLS_DHE_PSK_WITH_AES_256_GCM_SHA384

II. TLS curves:

i. X25519

ii. prime256v1 (also called secp256r1)

iii. secp384r1

III. Certificate type:

i. ECDSA (P-256) (recommended)

ii. RSA (2048 bits)

IV. Diffie-Hellman groups:

i. DH parameter size: 2048 (ffdhe2048, RFC 7919)

ii. Except curve25519, ed25519, and W-25519 (elliptic curve groups of less than 256 bits shall not be supported).

iii. For DHE, Diffie-Hellman groups of at least 4096 bits (Diffie-Hellman groups smaller than 2048 bits shall not be supported).

V. TLS hash algorithms :

i. SHA-256

ii. SHA-384

iii. ecdsa_secp384r1_sha384

VI. TLS signature algorithms:

i. ecdsa

ii. rsa_pss_rsae

iii. rsa_pkcs1 (not recommended)

iv. ecdsa_secp384r1_sha384

VII. The “null” compression method is mandatory to support.

VIII. HTTP Strict Transport Security (HSTS): max-age=63072000 (two years)

IX. Maximum certificate lifespan: 90 days (recommended) to 2 years

X. Cipher preference: client chooses

6.1.10.2 傳送層安全協定(TLS)的安全測試

(a) 測試依據:

依據 O-RAN Security Test Specification[15]之第 6.3 和 14.2 小節，並參考 O-RAN Security Protocols Specification[19]之第 2.2 小節。

(b) 測試目的:

驗證 SMO、Non-RT RIC、Near-RT RIC、O-CU、O-DU 與 O-RU 及 O-Cloud 間 A1 介面、O1 介面與 O2 介面的 TLS 協定受到安全保護。

(c) 測試前提:

(1) 待測物可以支援 TLS v1.2 或 TLS v1.3 的安全協定。

(2) 測試人員可採用分析工具或自動測試

i. 採用工具分析時，擷取 TLS 介面封包，並分析 TLS 協定內容。

ii. 採用自動測試時，需要透過 TLS 協定測試工具直接解密 A1 介面、O1 介面與 O2 介面封包，並分析封包內容。

(d) 測試佈局：

見圖 72。

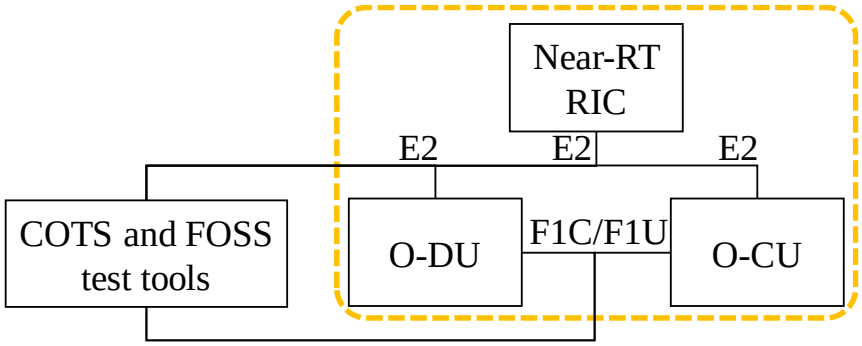


圖 72 傳送層安全協定(TLS)的安全測試測試示意圖

(e) 測試步驟:

(1) 待測物設定使用 TLS v1.2 或 TLS v1.3 的安全協定。

(2) 採用工具分析時，開始擷取 A1 介面、O1 介面與 O2 介面封包。

(3) 確認 O-DU 與 O-CU 建立 F1AP 連線，O-DU 和 O-CU 分別與 Near-RT RIC 建立 E2AP 連線，O-CU 與 5GC 建立 NGAP 連線，且用戶設備註冊上 5GC 並收送數據資料。

(4) 採用工具分析時，停止擷取 A1 介面、O1 介面與 O2 介面封包。

(5) 採用工具分析時，分析 A1 介面、O1 介面與 O2 介面封包，確認使用 TLS v1.2(或 TLS v1.3)的安全協定。採用自動測試時，由 TLS 協定測試工具確認。

i. 當使用 TLS v1.2 安全協定時，確認 TLS 安全協定使用之 TLS 1.2 中間密碼(Intermediate Ciphers for TLS 1.2)內容。

ii. 當使用 TLS v1.3 安全協定時，確認 TLS 1.3 中間密碼(Intermediate profile for TLS v1.3)或 TLS 1.3 現代密碼(Modern Ciphers for TLS 1.3)內容。

圖 73 傳送層安全協定(TLS)的安全測試測試流程圖

(f) 測試結果:

(1) 透過步驟(5)，待測物的 A1 介面、O1 介面與 O2 介面使用 TLS v1.2 或 TLS v1.3 的安全協定。

(2) 透過步驟(5)，確認待測物的 TLS 安全協定符合以下標準

[1] 當待測物使用 TLS 1.2 中間密碼(Intermediate Ciphers for TLS 1.2)安全協定時，其參數需要符合以下標準。

I. Cipher suites (TLS 1.2): (Only cipher suites with AEAD (e.g. GCM) and PFS (e.g. ECDHE, DHE) shall be supported)

i. TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

ii. TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

iii. TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

iv. TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

v. TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256

vi. TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256

vii. TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

viii. TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

ix. TLS_DHE_PSK_WITH_AES_128_GCM_SHA256

x. TLS_DHE_PSK_WITH_AES_256_GCM_SHA384

II. TLS curves:

i. X25519

ii. prime256v1 (also called secp256r1)

iii. secp384r1

III. Certificate type:

i. ECDSA (P-256) (recommended)

ii. RSA (2048 bits)

IV. Diffie-Hellman groups:

i. DH parameter size: 2048 (ffdhe2048, RFC 7919)

ii. Except curve25519, ed25519, and W-25519 (elliptic curve groups of less than 256 bits shall not be supported).

iii. For DHE, Diffie-Hellman groups of at least 4096 bits (Diffie-Hellman groups smaller than 2048 bits shall not be supported).

V. TLS hash algorithms :

i. SHA-256

ii. SHA-384

iii. ecdsa_secp384r1_sha384

VI. TLS signature algorithms:

i. ecdsa

ii. rsa_pss_rsae

iii. rsa_pkcs1 (not recommended)

iv. ecdsa_secp384r1_sha384

VII. The “null” compression method is mandatory to support.

VIII. HTTP Strict Transport Security (HSTS): max-age=63072000 (two years)

IX. Maximum certificate lifespan: 90 days (recommended) to 2 years

X. Cipher preference: client chooses

[2] 當待測物使用 TLS 1.3 中間密碼(Intermediate Ciphers for TLS 1.3)安全協定時，其參數需要符合以下標準。

I. Cipher suites (TLS 1.3):

i. TLS_AES_128_GCM_SHA256

ii. TLS_AES_256_GCM_SHA384

iii. TLS_CHACHA20_POLY1305_SHA256

II. TLS curves:

i. X25519

ii. prime256v1

iii. secp384r1

III. Certificate type:

i. ECDSA (P-256) (recommended)

ii. RSA (2048 bits)

IV. DH parameter size: 2048 (ffdhe2048, RFC 7919)

V. The requirements given in section 9.1 of TLS 1.3 RFC 8446 shall be followed.

i. Key exchange with secp384r1 should be supported.

VI. TLS signature schemes:

i. ecdsa_secp384r1_sha384

VII. TLS extensions: (The requirements given in section 9.2 of TLS 1.3 RCF 8446 shall be followed)

i. The OCSP Status extension (a.k.a. certificate status request), as defined in RFC 6066 and RFC 8446 should be supported.

VIII. HTTP Strict Transport Security (HSTS): max-age=63072000 (two years)

IX. Maximum certificate lifespan: 90 days (recommended) to 2 years

X. Cipher preference: client chooses

[3] 當待測物使用 TLS 1.3 現代密碼(Modern Ciphers for TLS 1.3)安全協定時，其參數需要符合以下標準。

I. Cipher suites (TLS 1.3):

i. TLS_AES_128_GCM_SHA256

ii. TLS_AES_256_GCM_SHA384

iii. TLS_CHACHA20_POLY1305_SHA256

II. Certificate type: ECDSA (P-256)

III. TLS curves:

i. X25519

ii. prime256v1

iii. secp384r1

IV. The requirements given in section 9.1 of TLS 1.3 RFC 8446 shall be followed.

i. Key exchange with secp384r1 should be supported.

V. TLS signature schemes:

i. ecdsa_secp384r1_sha384.

VI. TLS extensions: (The requirements given in section 9.2 of TLS 1.3 RFC 8446 shall be followed.)

i. The OCSP Status extension (a.k.a. certificate status request), as defined in RFC 6066 and RFC 8446 should be supported.

VII. HSTS: max-age=63072000 (two years)

VIII. Maximum certificate lifespan: 90 days

IX. Cipher preference: client chooses

6.1.10.3 OAuth 2.0 的安全測試

(a) 測試依據：

參考 O-RAN Security Test Specification[15]之第 6.6 小節。

(a) 測試目的：

驗證 Non-RT RIC 與 Near-RT RIC 的應用服務 rAPP 與 xAPP 能夠支援 OAuth 2.0 的安全防護。

(b) 測試前提：

(1) Non-RT RIC 與 Near-RT RIC 可以支援 OAuth 2.0 的安全防護。

(2) 應用服務取得符記(token)的流程支援交互傳送層安全(Mutual Transport Layer Security, mTLS)驗證。

(3) 以符記(token)為基礎的應用服務存取支援交互傳送層安全(Mutual Transport Layer Security, mTLS)驗證。

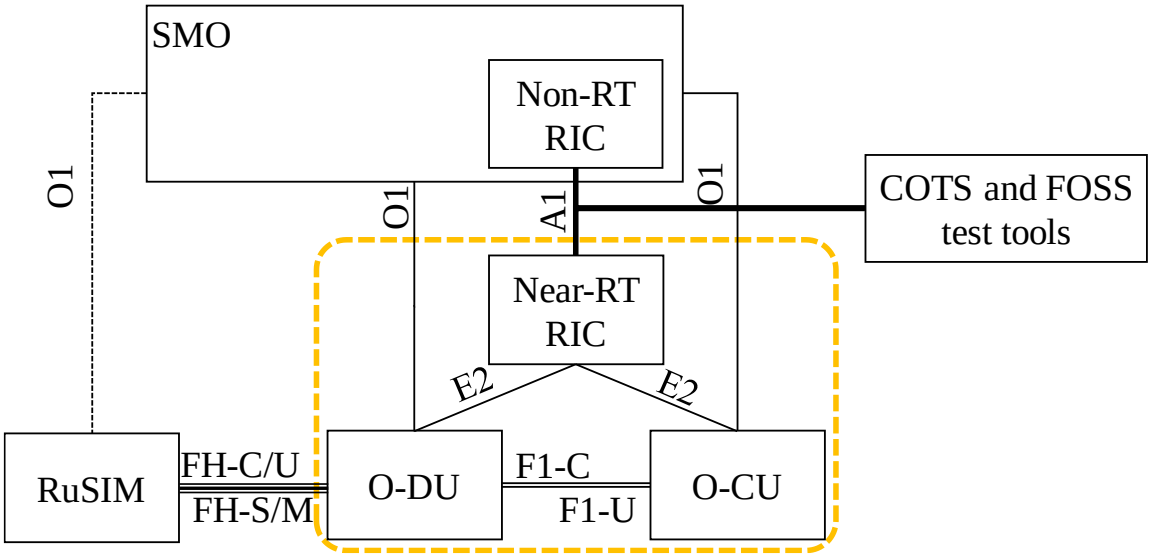
(4) 測試人員可採用分析工具或自動測試。

i. 採用工具分析時，擷取 A1 介面封包，並分析 A1 介面的封包內容。

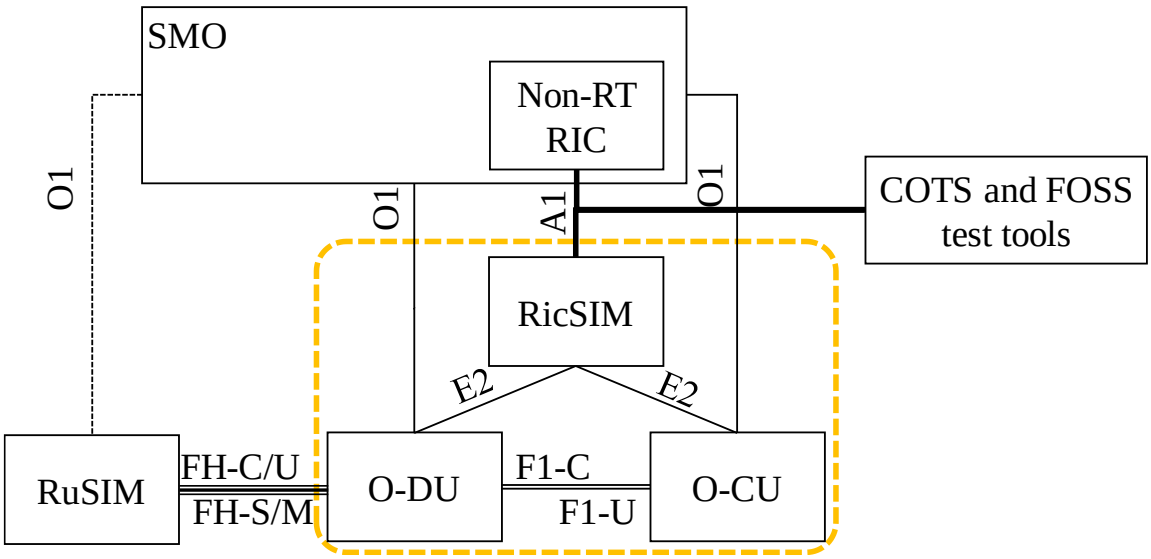
ii. 採用自動測試時，需要透過 RicSIM 解密 A1 介面封包，並分析封包內容。

(c) 測試佈局：

見圖 74。



(a) 使用 RuSIM 與 RicSIM 測試



(b) 使用 RuSIM 測試

圖 74 應用服務的 OAuth 2.0 安全防護測試示意圖

(d) 測試步驟：

(1) 採用工具分析時，開始擷取 A1 介面封包。

(2) 透過 A1 介面對 OAuth 2.0 伺服器發送交互傳送層安全(mTLS)驗證的符記(token)請求信令，該信令包含如下設定。

i. 合法的用戶端認證與正確的參數

ii. 非法的用戶端認證

iii. 合法的用戶端認證與不正確的參數。

(3) 採用工具分析時，停止擷取 A1 介面封包。

(4) 採用工具分析時，需要分析 A1 介面封包，確認與 OAuth 2.0 伺服器安全連線建立的結果。採用自動測試時，由 RicSIM 確認。

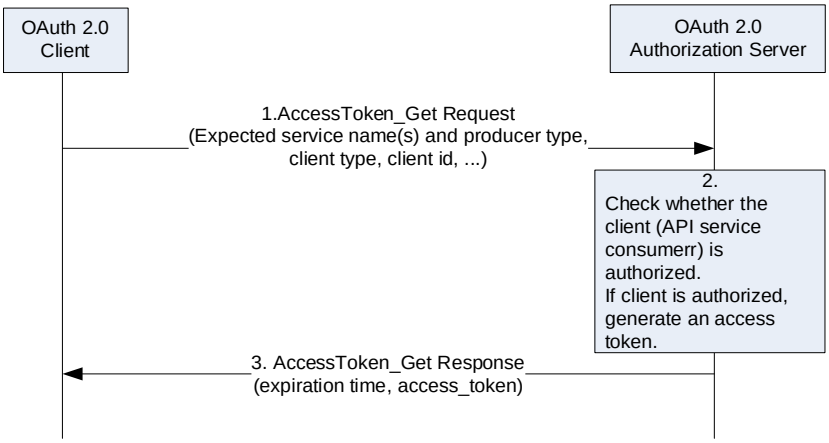


圖 75 OAuth 2.0 的安全防護測試流程圖

(5) 採用工具分析時，開始擷取 A1 介面封包。

(6) 透過 A1 介面分別使用合法符記(token)與非法符記(token)對應用服務發送交互傳送層安全(mTLS)驗證的服務請求(service request)信令。

(7) 採用工具分析時，停止擷取 A1 介面封包。

(8) 採用工具分析時，需要分析 A1 介面封包，確認與應用服務建立安全連線並獲得回應。採用自動測試時，由 RicSIM 確認。

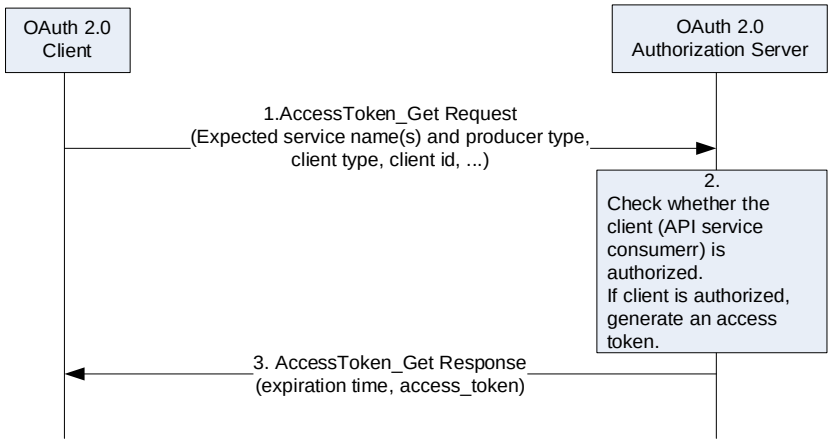


圖 76 應用服務安全防護測試流程圖

(e) 測試結果：

(1) 根據步驟(4)，當對 OAuth 2.0 伺服器發送符記(token)請求信令包含合法的用戶端認證與正確的參數時，能夠成功與伺服器建立連線並取得受到網頁簽章(JSON Web Signature, JWS)保護的符記(token)。

(2) 根據步驟(4)，當對 OAuth 2.0 伺服器發送符記(token)請求信令包含非法的用戶端認證時，與 OAuth 2.0 伺服器建立連線會失敗。

(3) 根據步驟(4)，當對 OAuth 2.0 伺服器發送符記(token)請求信令包含合法的用戶端認證與不正確的參數時，能夠成功與 OAuth 2.0 伺服器建立連線，但無法取得符記(token)。

(4) 根據步驟(8)，當使用合法符記(token)發送服務請求(service request)信令時，確認與應用服務成功建立連，並獲得回應(resonse)信令。

(5) 根據步驟(8)，當使用非法符記(token)發送服務請求(service request)信令時，確認與應用服務成功建立連，並獲得失敗回應(failed resonse)信令(401)。

6.1.11 RIC 介面功能安全性檢測

6.1.11.1 A1 介面模糊測試(非必測項目)

(a) 測試依據:

依據 O-RAN TIFG E2E-Test [20]之第 7.2.6 小節。

(b) 測試目的:

驗證當 Near-RT RIC 的 A1 介面遭受非預期訊號攻擊時，Near-RT RIC 的性能不會受到影響。

(c) 測試前提:

(1) Near-RT RIC 通過 O-RAN TIFG E2E-Test [17]之第 5.6 小節與第 6.1 小節的測試項目。

(2) UE、O-RU、O-DU、O-CU 及 5GC 端可成功建立 5G 連線。

(3) Non-RT RIC 模糊測試器能夠連接到 Near-RT RIC 的 A1 介面。

(d) 測試佈局：

見圖 32。

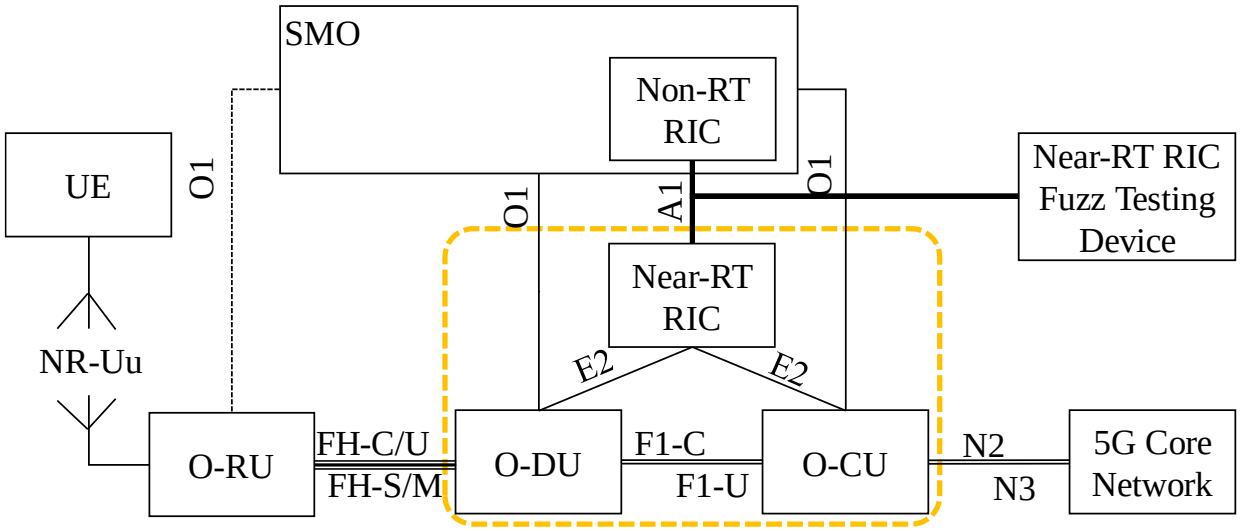


圖 77 A1 介面模糊測試示意圖

(e) 測試步驟:

(1) Non-RT RIC 模糊測試器對於 Near-RT RIC 的 A1 介面產生超文件傳輸協定(HyperText Transfer Protocol, HTTP)或超文件傳輸安全協定(HyperText Transfer Protocol Secure, HTTPs)的表現層狀態轉換(REpresentational State Transfer, REST) (APplication Interface, API)應用介面信令之非預期訊號攻擊封包。

(2) Non-RT RIC 模糊測試器產生 250,000 次的非預期訊號攻擊流量。

(3) 對 Near-RT RIC 實施 O-RAN TIFG E2E-Test [17]之第 5.6 小節與第 6.1 小節的測試項目。

(f) 測試結果:

(1) 根據步驟(4)，確認 Near-RT RIC 的性能不會受到影響。

6.1.11.2 A1 介面阻斷服務測試(非必測項目)

(a) 測試依據:

依據 O-RAN TIFG E2E-Test [20]之第 7.2.3 小節。

(b) 測試目的:

驗證當 Near-RT RIC 的 A1 介面遭受非預期訊號攻擊時，Near-RT RIC 的性能不會受到影響。

(c) 測試前提:

(1) Near-RT RIC 通過 O-RAN TIFG E2E-Test [17]之第 5.6 小節與第 6.1 小節的測試項目。

(2) UE、O-RU、O-DU、O-CU 及 5GC 端可成功建立 5G 連線。

(3) Non-RT RIC 阻斷服務攻擊模擬器能夠連接到 Near-RT RIC 的 A1 介面。

(d) 測試佈局：

見圖 78。

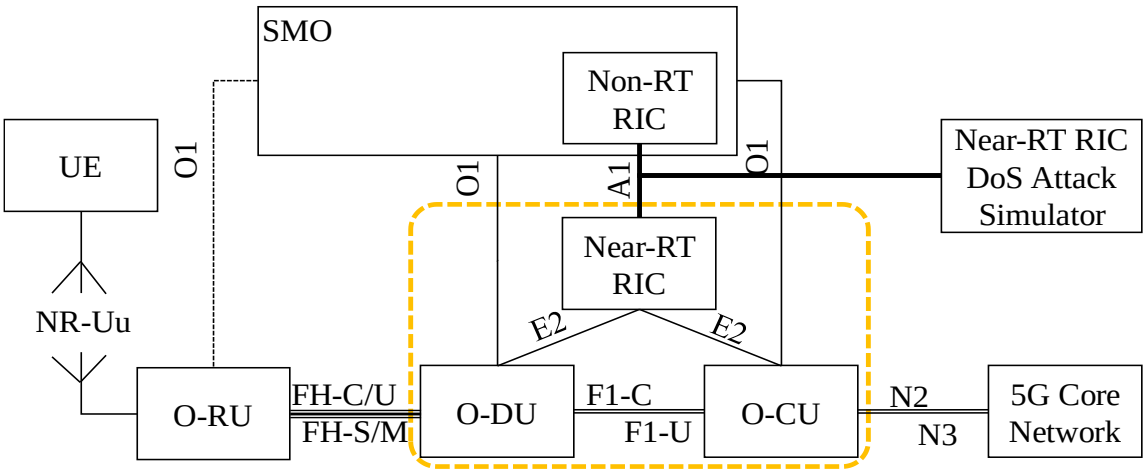


圖 78 A1 介面阻斷服務測試示意圖

(e) 測試步驟:

(1) Non-RT RIC 阻斷服務攻擊模擬器對於 Near-RT RIC 的 A1 介面產生超文件傳輸協定(HyperText Transfer Protocol, HTTP)或超文件傳輸安全協定(HyperText Transfer Protocol Secure, HTTPs)的表現層狀態轉換(REpresentational State Transfer, REST) (APplication Interface, API)應用介面信令之阻斷服務攻擊封包。

(2) Non-RT RIC 阻斷服務攻擊模擬器的攻擊流量為 10Mbps、100Mbps 與 1Gbps。

(3) Non-RT RIC 阻斷服務攻擊模擬器產生之攻擊封包的媒體存取控制位址(MAC address) 須為篡改的 PTPGM 位址、隨機位址和廣播位址。

(4) 對 O-DU 實施 O-RAN TIFG E2E-Test [17]之第 5.6 小節與第 6.1 小節的測試項目。

(f) 測試結果:

(1) 根據步驟(4)，確認 Near-RT RIC 的性能不會受到影響。

6.1.11.3 分散式阻斷服務攻擊測試

(a) 測試依據：

依據 O-RAN Security Test Specification [12] 之第 7.5.1 小節。

(b) 測試目的：

確認 O-RAN 系統能夠防止分散式阻斷服務 (Distributed Denial-of-Service, DDoS) 攻擊。

(c) 測試前提：

(1) 測試人員能夠透過 O-RAN 系統的介面進行分散式阻斷服務(DDoS)攻擊測試。

(d) 測試佈局：

見圖 79。

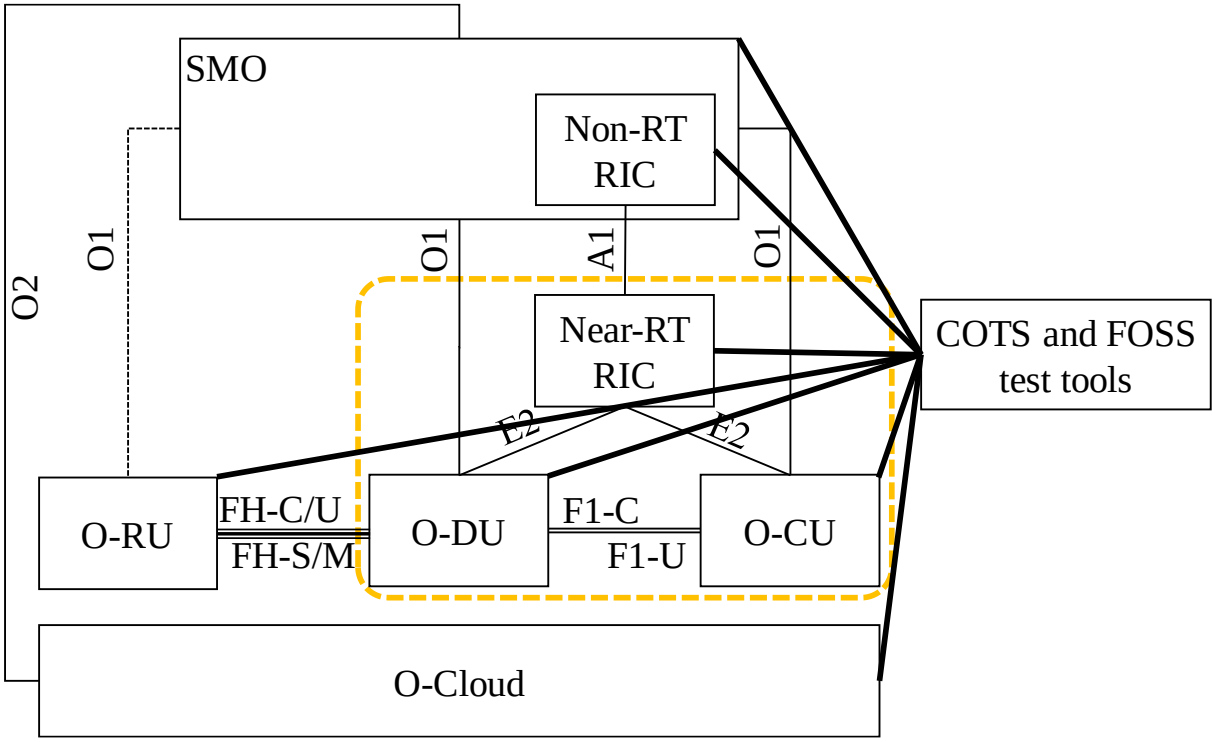


圖 79 分散式阻斷服務攻擊測試示意圖

(e) 測試步驟：

(1) 針對 O-RAN 系統發送協定層攻擊 (Protocol Layer Attacks) 與大量洪水攻擊 (Volume based Attacks) 以及應用層攻擊 (Application Layer Attacks)。

(2) 協定層攻擊 (Protocol Layer Attacks) 涵蓋請求洪水攻擊 (SYN Floods Attack)、網際連結控制信息協定回音檢查破滅攻擊 (Ping of Death Attack) 與分散式阻斷攻擊 (Smurf DDoS) 攻擊等。

(3) 大流量攻擊 (Volume based Attacks) 涵蓋用戶資料元協定洪水攻擊(UDP Floods Attack)攻擊，網際連結控制信息協定洪水攻擊(ICMP Floods Attack)攻擊等。

(4) 應用層攻擊 (Application Layer Attacks) 涵蓋 GET/POST 洪水攻擊(GET/POST Floods Attack)、低速緩慢攻擊 (Low and Slow Attack)、針對 Apache 攻擊、針對 Windows 攻擊或針對 OpenBSD 攻擊等。

(5) 確認 O-RAN 系統當機時間。

(6) 確認對外部服務無反應時間。

(f) 測試結果：

(1) 根據步驟(5)與(6)，確認 O-RAN 系統不會當機或對外部服務無反應。

6.2 系統與應用服務安全

6.2.1 資料安全

6.2.1.1 系統功能造成敏感資料外洩

依據 TAICS TS-0035 5G 基地臺資安測試規範的 6.2.1.1 節定義之測試流程。

6.2.1.2 韌體造成敏感資料外洩

依據 TAICS TS-0035 5G 基地臺資安測試規範的 6.2.1.2 節定義之測試流程。

6.2.1.3 確保敏感性資料進行加密處理再儲存

依據 TAICS TS-0035 5G 基地臺資安測試規範的 6.2.1.3 節定義之測試流程。

6.2.2 應用程式安全

6.2.2.1 網站伺服器不存在常見之網路應用系統安全弱點

依據 TAICS TS-0035 5G 基地臺資安測試規範的 6.2.2.1 節定義之測試流程。

6.2.2.2 系統使用之協定與服務採最小化設計

依據 TAICS TS-0035 5G 基地臺資安測試規範的 6.2.2.2 節定義之測試流程。

6.2.2.3 網路傳輸過程使用加密技術確保資料安全

依據 TAICS TS-0035 5G 基地臺資安測試規範的 6.2.2.3 節定義之測試流程。

6.2.2.4 網際網路安全協定(IPsec)已知弱點掃描

(a) 測試依據:

依據 O-RAN Security Test Specification[15]之第 6.4 小節，並參考 O-RAN Security Protocols Specification[19]之第 2.4 小節。

(b) 測試目的:

驗證待測物的安全閘道器(Security Gateway, SeGW)不應存在已知弱點。

(c) 測試前提:

(1) 待測物的安全閘道器(SeGW)可以支援 IKEv2 的安全協定。

(2) 測試人員可以對待測物的安全閘道器(SeGW)進行 IPsec 協定弱點掃描。

(d) 測試佈局：

見圖 80。

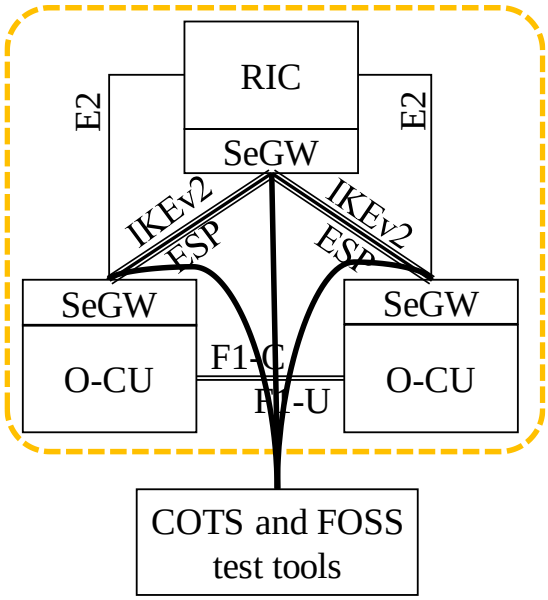


圖 80 網際網路安全協定(IPsec)的已知弱點掃描示意圖

(e) 測試步驟:

(1) 待測物設定使用第二版(v2)的 IKEv2 安全協定。

(2) 對待測物的安全閘道器(SeGW)進行 IPsec 協定弱點掃描。

(f) 測試結果:

(1) 透過步驟(6)，弱點掃描後未發現任何安全閘道器(SeGW)的 IPsec 協定已知弱點(well-known vulnerabilities)。

6.2.2.5 安全外殼協定(SSH)已知弱點掃描

(a) 測試依據:

依據 O-RAN Security Test Specification[15]之第 6.2 小節，並參考 O-RAN Security Protocols Specification[19]之第 2.1 小節。

(b) 測試目的:

驗證 O-RU 與 O-DU 之 Open FH 介面 M-plane 的 SSH 協定不應存在已知弱點。

(c) 測試前提:

(1) SSH 協定測試工具可以透過 Open FH 介面 M-plane 與 O-RU 與 O-DU 建立 SSH 連線。

(2) SSH 協定測試工具可以模擬 SSH 協定用戶端與 SSH 協定伺服器。

(3) 測試人員可以對 Open FH 介面 M-plane 進行 SSH 協定弱點掃描。

(d) 測試佈局：

見圖 81。

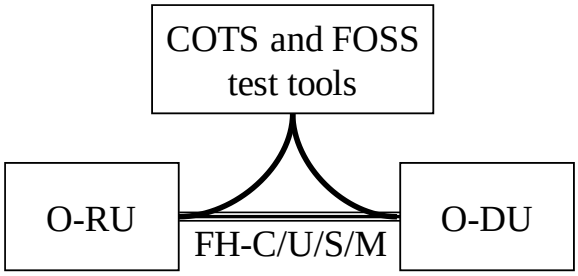


圖 81 安全外殼協定(SSH)的已知弱點掃描示意圖

(e) 測試步驟:

(1) 待測物設定使用第二版(v2)的 SSH 安全協定。

(2) 透過 Open FH 介面 M-plane 對待測物進行 SSH 協定弱點掃描。

(f) 測試結果:

(1) 透過步驟(2)，弱點掃描後未發現任何 SSH 協定已知弱點(well-known vulnerabilities)。

6.2.2.6 資料包傳送層安全協定(DTLS)已知弱點掃描(使用 IPsec 時無須測試)

(a) 測試依據:

依據 O-RAN Security Test Specification[15]之第 6.4 小節，並參考 O-RAN Security Protocols Specification[19]之第 2.4 小節。

(b) 測試目的:

驗證待測物的安全閘道器(Security Gateway, SeGW)不應存在已知弱點。

(c) 測試前提:

(1) 待測物的安全閘道器(SeGW)可以支援 DTLS v1.2 的安全協定。

(2) 測試人員可以對待測物的安全閘道器(SeGW)進行 DTLS 協定弱點掃描。

(d) 測試佈局：

見圖 6。

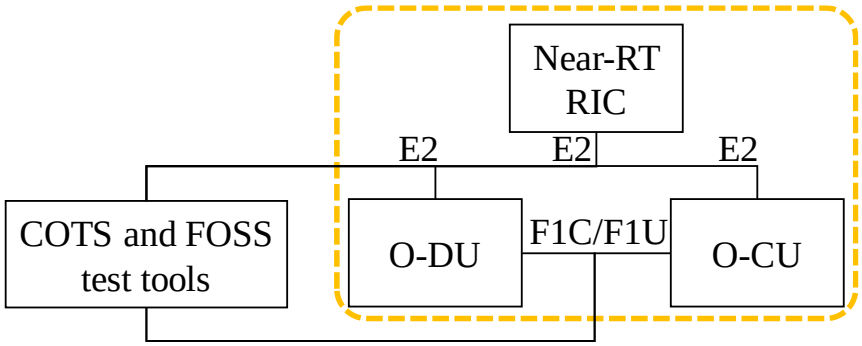


圖 82 資料包傳送層安全協定(DTLS)的已知弱點掃描示意圖

(e) 測試步驟:

(1) 待測物的安全閘道器(SeGW)設定使用 DTLS v1.2 安全協定。

(2) 對待測物的安全閘道器(SeGW)進行 DTLS 協定弱點掃描。

(f) 測試結果:

(1) 透過步驟(6)，弱點掃描後未發現任何待測物的安全閘道器(SeGW)的 DTLS 協定已知弱點(well-known vulnerabilities)。

6.2.2.7 傳送層安全協定(TLS)的安全測試已知弱點掃描

(a) 測試依據:

依據 O-RAN Security Test Specification[15]之第 6.3 和 14.2 小節，並參考 O-RAN Security Protocols Specification[19]之第 2.2 小節。

(b) 測試目的:

驗證 SMO、Non-RT RIC、Near-RT RIC、O-CU、O-DU 與 O-RU 及 O-Cloud 間 A1 介面、O1 介面與 O2 介面的 TLS 協定不應存在已知弱點。

(c) 測試前提:

(1) 待測物可以支援 TLS v1.2 或 TLS v1.3 的安全協定。

(2) 測試人員可以對 A1 介面、O1 介面與 O2 介面進行 TLS 協定弱點掃描。

(d) 測試佈局：

見圖 6。

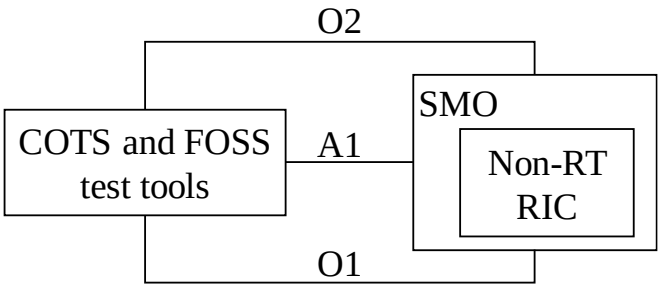


圖 83 傳送層安全協定(TLS)的已知弱點掃描示意圖

(e) 測試步驟:

(1) 待測物設定使用 TLS v1.2 或 TLS v1.3 的 TLS 安全協定。

(2) 透過 A1 介面、O1 介面與 O2 介面對待測物進行 TLS 協定弱點掃描。

(f) 測試結果:

(1) 透過步驟(6)，弱點掃描後未發現任何 TLS 協定已知弱點(well-known vulnerabilities)。

6.2.2.8 A1 介面已知弱點掃描(非必測項目)

(a) 測試依據：

依據 O-RAN TIFG E2E-Test [20]之第 7.2.7 小節。

(b) 測試目的：

Near-RT RIC 的 A1 介面不應存在重大風險已知弱點漏洞，驗證是否存在中高風險已知弱點。

(c) 測試前提：

(1) 測試人員能夠透過 Near-RT RIC 的 A1 介面進行已知弱點漏洞掃描。

(d) 測試佈局：

見圖 84。

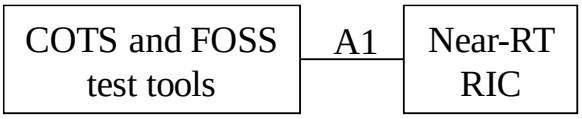


圖 84 作業系統及網路服務安全測試示意圖

(e) 測試步驟：

(1) 將測試電腦連接受測系統。

(2) 啟動弱點掃描功能之工具，對 Near-RT RIC 的 A1 介面執行弱點掃描。

(3) 檢視該弱點掃描工具所產生之報告，是否存在 CVSS v3 評分為 7 分以上之資安漏洞。

(f) 測試結果：

Near-RT RIC 的 A1 介面不存在 CVSS v3 評分為最高風險 7 分以上之高風險資安漏洞，若無 CVSS v3 評分則採用 CVSS v2 評分方式。

6.2.2.9 網路服務列舉

(a) 測試依據：

依據 O-RAN Security Test Specification [15] 之第 7.2.1 小節。

(b) 測試目的：

實際維運階段預設只執行 O-RAN 供應商需要的協定和服務，確保未知的協定與服務在管理者不知情下運行。

(c) 測試前提：

O-RAN 供應商應提供以下書面資料作為審查與檢測依據：

(1) 提供 SMO、Non-RT RIC、Near-RT RIC、O-CU、O-DU、O-RU、O-Cloud 實際維運階段所需預設開啟之協定與服務用途列表。

(d) 測試佈局：

見圖 85。

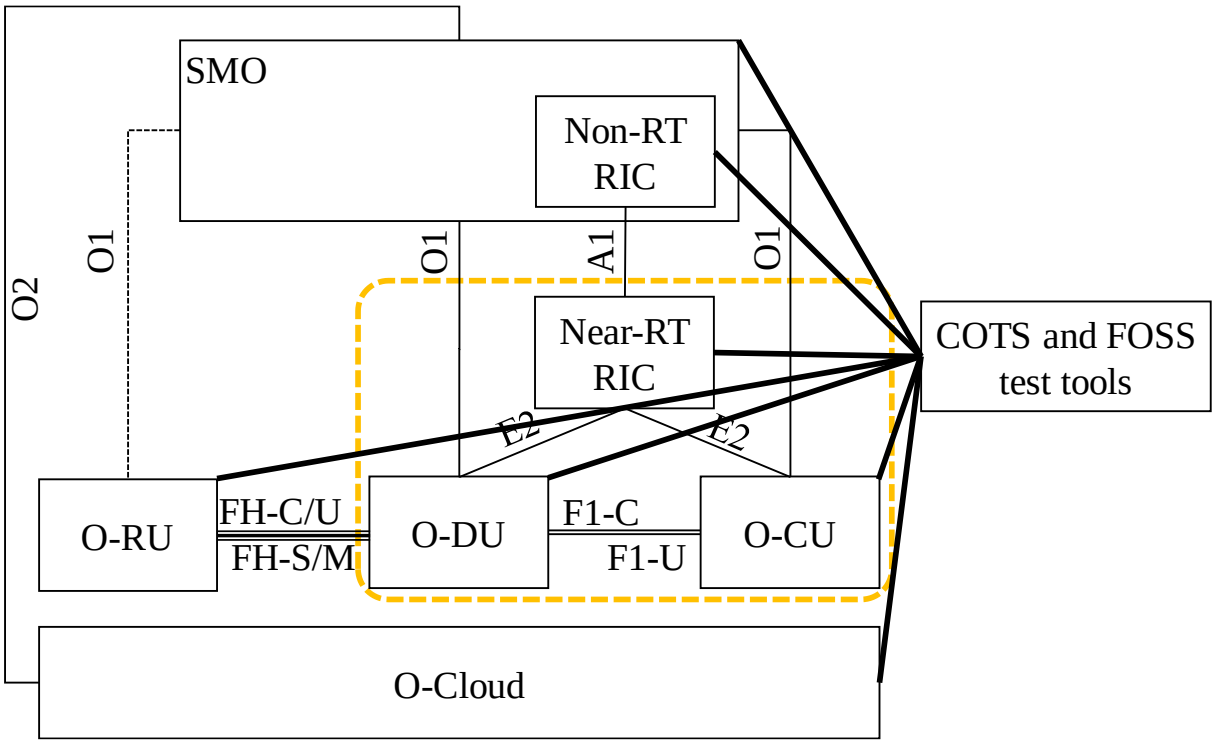


圖 85 O-RAN 基地臺使用之協定與服務採最小化設計測試示意圖

(e) 測試步驟：

(1) 使用埠掃瞄工具檢測受測系統運行的服務列表。

(2) 掃瞄之服務涵蓋傳輸控制協定(Transmission Control Protocol, TCP)與用戶資料元協定(User Datagram Protocol, UDP)及串流控制傳輸協定(Stream Control Transmission Protocol, SCTP) 。

(3) 確認服務列表中的服務為 O-RAN 供應商實際維運階段所需協定與服務。

(4) 重啟 O-RAN 基地臺，重新執行步驟(1)至步驟(2)，確認服務列表中的服務為 O-RAN 供應商實際維運階段所需協定與服務。

(5) 評估所有開啟之協定與服務的合理與必要性。

(f) 測試結果：

步驟(2)與步驟(3)中，確認與 O-RAN 供應商自我宣告表一致。步驟(4)，確認開啟之服務都有其合理與必要性。

6.2.3 身分鑑別與授權

6.2.3.1 禁止未經認證與授權使用系統各項功能

依據 TAICS TS-0035 5G 基地臺資安測試規範的 6.2.3.1 節定義之測試流程。

6.2.3.2 每一個帳號至少要有一個身分鑑別因子方可鑑別成功

依據 TAICS TS-0035 5G 基地臺資安測試規範的 6.2.3.2 節定義之測試流程。

6.2.3.3 系統預設帳號應可移除或設置停用

依據 TAICS TS-0035 5G 基地臺資安測試規範的 6.2.3.3 節定義之測試流程。

6.2.3.4 系統應支援與設定不同組合之密碼複雜性規格

依據 TAICS TS-0035 5G 基地臺資安測試規範的 6.2.3.4 節定義之測試流程。

6.2.3.5 密碼變更機制

依據 TAICS TS-0035 5G 基地臺資安測試規範的 6.2.3.5 節定義之測試流程。

6.2.3.6 系統應具備暴力及字典攻擊的防護措施

依據 TAICS TS-0035 5G 基地臺資安測試規範的 6.2.3.6 節定義之測試流程。

6.2.3.7 密碼顯示遮罩

依據 TAICS TS-0035 5G 基地臺資安測試規範的 6.2.3.7 節定義之測試流程。

6.2.3.8 密碼連續輸入錯誤處理

依據 TAICS TS-0035 5G 基地臺資安測試規範的 6.2.3.8 節定義之測試流程。

6.2.3.9 授權策略

依據 TAICS TS-0035 5G 基地臺資安測試規範的 6.2.3.9 節定義之測試流程。

6.2.3.10 O-RAN 基地臺應支援基於角色之存取控制

依據 TAICS TS-0035 5G 基地臺資安測試規範的 6.2.3.10 節定義之測試流程。

6.2.3.11 登出功能是否有效

依據 TAICS TS-0035 5G 基地臺資安測試規範的 6.2.3.11 節定義之測試流程。

6.2.3.12 登入之權限控管

依據 TAICS TS-0035 5G 基地臺資安測試規範的 6.2.3.12 節定義之測試流程。

6.2.3.13 檔案系統存取權限控管

依據 TAICS TS-0035 5G 基地臺資安測試規範的 6.2.3.13 節定義之測試流程。

6.2.3.14 O-RAN 基地臺應支援操作逾時功能

依據 TAICS TS-0035 5G 基地臺資安測試規範的 6.2.3.14 節定義之測試流程。

6.2.3.15 暴力破解

(a) 測試依據：

依據 O-RAN Security Test Specification [15] 之第 7.3.1 小節。

(b) 測試目的：

系統應避免使用通用密碼，確保系統避免遭受密碼暴力攻擊破解的風險。

(c) 測試前提：

O-RAN 供應商應提供以下書面資料作為審查與檢測依據：

(1) 提供 SMO、Non-RT RIC、Near-RT RIC、O-CU、O-DU、O-RU、O-Cloud 密碼登入之操作文件。

(d) 測試佈局：

見圖 86。

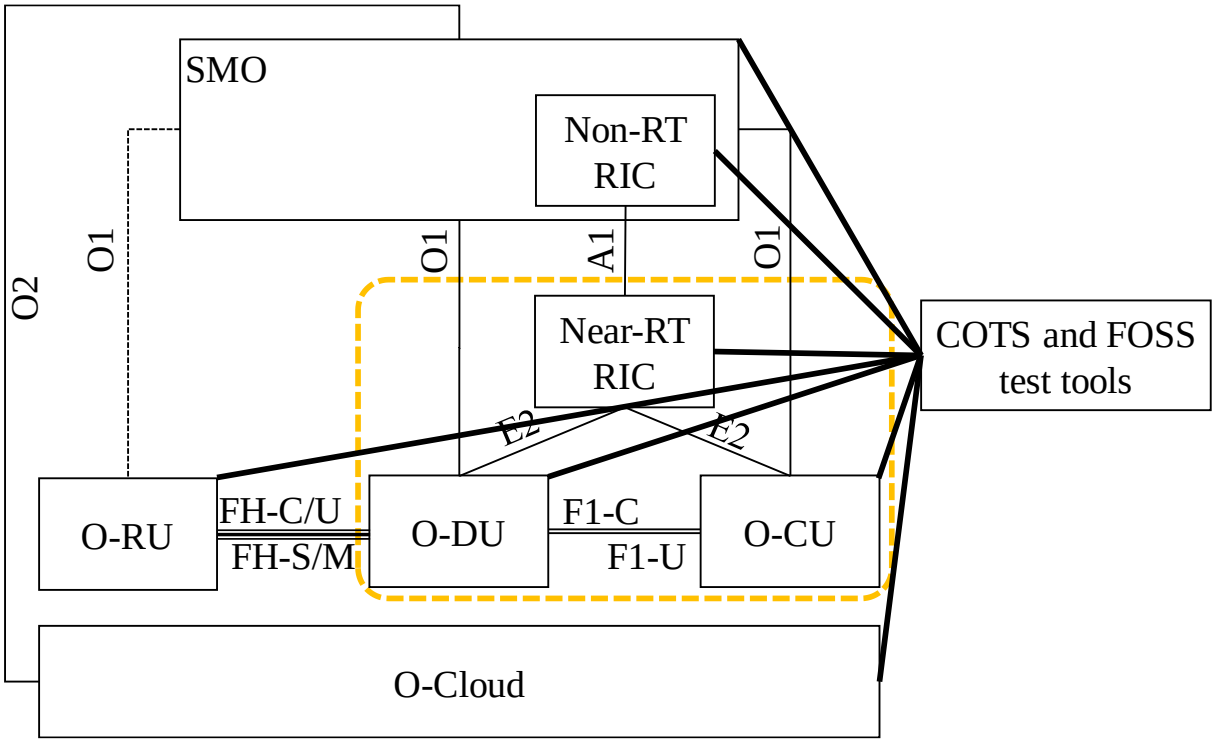


圖 86 複雜性規格測試示意圖

(g) 測試步驟：

(1) 開啟受測系統登入畫面。

(2) 測試人員使用通用密碼登入任一個系統帳號。

(h) 測試結果：

步驟(2)中，確認無法使用通用密碼登入任一個系統帳號。

6.2.3.16 未經授權的密碼重置

(a) 測試依據：

依據 O-RAN Security Test Specification [15] 之第 7.3.2 小節。

(b) 測試目的：

系統應禁止未經硬體系統重置密碼，確保系統避免遭受密碼暴力攻擊破解的風險。

(c) 測試前提：

O-RAN 供應商應提供以下書面資料作為審查與檢測依據：

(1) 提供 SMO、Non-RT RIC、Near-RT RIC、O-CU、O-DU、O-RU、O-Cloud 的硬體系統重置之操作文件。

(d) 測試佈局：

見圖 87。

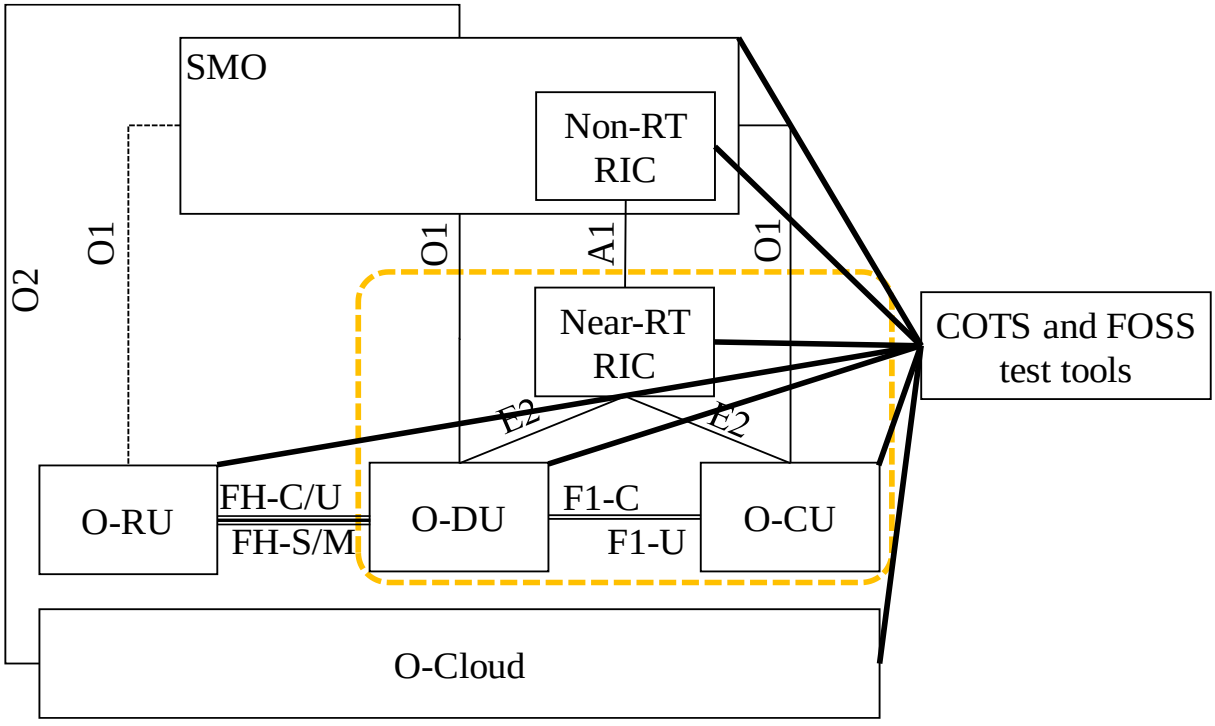


圖 87 密碼複雜性規格測試示意圖

(e) 測試步驟：

(1) 啟動硬體系統重置。

(2) 測試人員使用預設帳號登入系統。

(f) 測試結果：

步驟(2)中，確認啟動硬體系統重置後，無法使用預設帳號登入系統。

6.2.3.17 強制密碼政策

(a) 測試依據：

依據 O-RAN Security Test Specification [15] 之第 7.3.3 小節。

(b) 測試目的：

系統應支援與設定不同組合之密碼複雜性規格(長度、英文大小寫、數字、符號)，確保系統避免遭受密碼暴力攻擊破解的風險。

(c) 測試前提：

O-RAN 供應商應提供以下書面資料作為審查與檢測依據：

(1) 提供 SMO、Non-RT RIC、Near-RT RIC、O-CU、O-DU、O-RU、O-Cloud 密碼修改之操作文件。

(d) 測試佈局：

見圖 88。

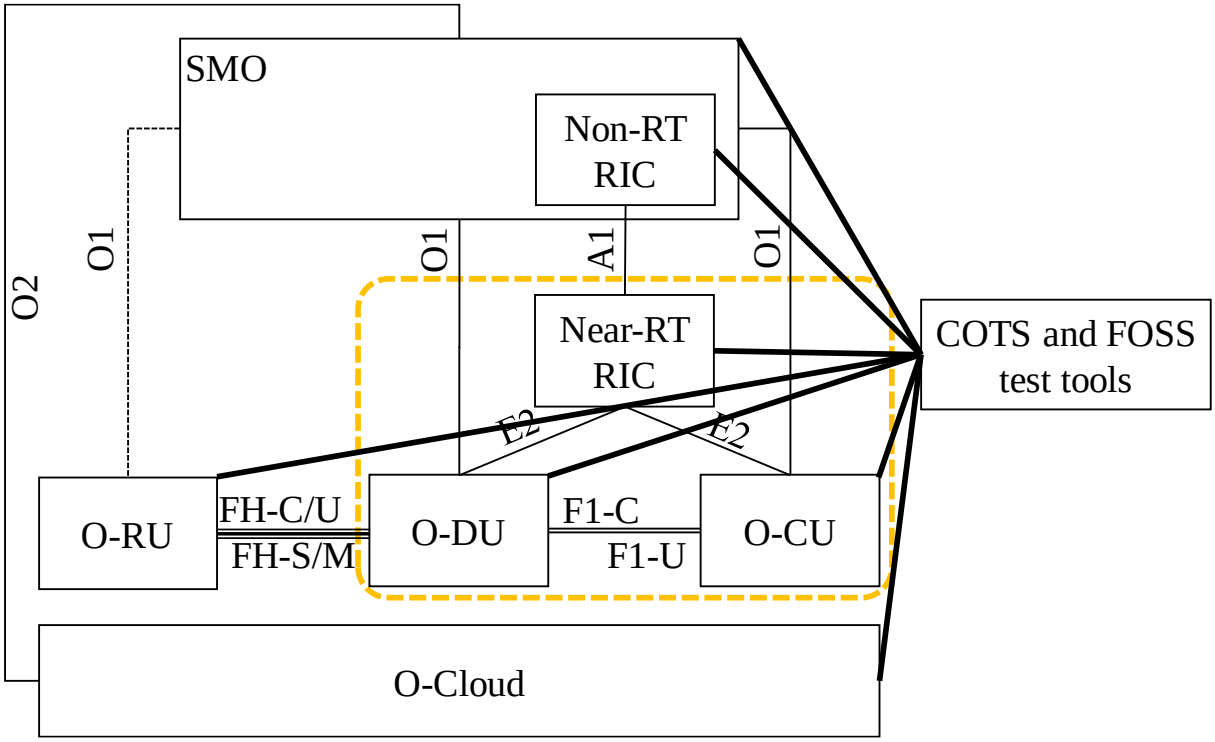


圖 88 強制密碼政策測試示意圖

(e) 測試步驟：

(1) 開啟受測系統登入畫面。

(2) 測試人員使用管理員帳號登入系統，並將密碼複雜度規格套用至特定帳號。

(3) 測試人員使用已修改密碼複雜度規則之帳號登入系統。

(f) 測試結果：

步驟(2)中，確認系統可將密碼複雜度規則套用至特定帳號。步驟(3)中，確認帳號可以正常登入至系統。

6.2.4 作業系統安全

6.2.4.1 日誌檔不能洩露個人資料

依據 TAICS TS-0035 5G 基地臺資安測試規範的 6.2.4.1 節定義之測試流程。

6.2.4.2 開機僅可透過合法的韌體

依據 TAICS TS-0035 5G 基地臺資安測試規範的 6.2.4.2 節定義之測試流程。

6.2.4.3 O-RAN 基地臺應具備軟體完整性自我檢測機制

依據 TAICS TS-0035 5G 基地臺資安測試規範的 6.2.4.3 節定義之測試流程。

6.2.4.4 系統應提供安全事件記錄功能

依據 TAICS TS-0035 5G 基地臺資安測試規範的 6.2.4.4 節定義之測試流程。

6.2.4.5 系統應提供可將安全事件記錄功能轉移備存至外部系統

依據 TAICS TS-0035 5G 基地臺資安測試規範的 6.2.4.5 節定義之測試流程。

6.2.4.6 O-RAN 基地臺的安全事件紀錄應有存取控制限制

依據 TAICS TS-0035 5G 基地臺資安測試規範的 6.2.4.6 節定義之測試流程。

6.2.4.7 確保高權限的系統功能必須經過身分鑑別

依據 TAICS TS-0035 5G 基地臺資安測試規範的 6.2.4.7 節定義之測試流程。

6.2.4.8 可卸除儲存媒體禁止啟用自動播放功能

依據 TAICS TS-0035 5G 基地臺資安測試規範的 6.2.4.8 節定義之測試流程。

6.2.4.9 作業系統及網路服務安全

依據 TAICS TS-0035 5G 基地臺資安測試規範的 6.2.4.9 節定義之測試流程。

6.2.5 Open RAN 系統安全

6.2.5.1 O-Cloud 虛擬化安全

(a) 測試依據：

依據 O-RAN TIFG E2E-Test [20]之第 7.3 小節。

(b) 測試目的：

確認當 O-RAN 遭受資源耗盡的旁通道阻斷服務攻擊 (noisy neighbor DoS attack) 時，O-Cloud 的性能不會受到影響。

(c) 測試前提：

(1) O-Cloud 通過 O-RAN TIFG E2E-Test [17]之第 5.6 小節與第 6.1 小節的測試項目。

(2) UE、O-RU、O-DU、O-CU 及 5GC 端可成功建立 5G 連線。

(3) O-Cloud 阻斷服務攻擊模擬器能夠連接到 O-Cloud 的 O2 介面。

(d) 測試佈局：

見圖 89。

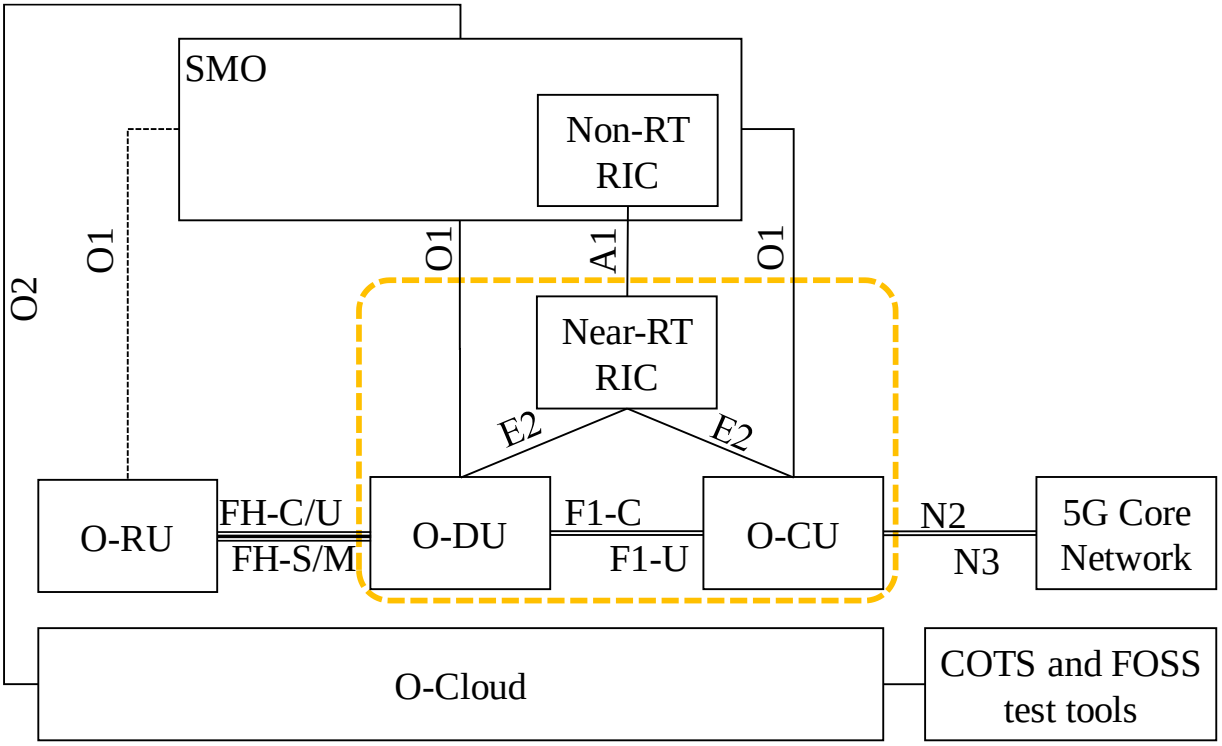


圖 89 O-Cloud 安全測試示意圖

(e) 測試步驟：

(1) O-Cloud 阻斷服務攻擊模擬器對於 O-Cloud 的 O2 介面產生資源耗盡的旁通道阻斷服務攻擊 (noisy neighbor DoS attack)。

(2) 對 O-DU 實施 O-RAN TIFG E2E-Test [17]之第 5.6 小節與第 6.1 小節的測試項目。

(f) 測試結果：

(1) 根據步驟(2)，確認 O-Cloud 的性能不會受到影響。

6.2.5.2 軟體物料清單簽章

(a) 測試依據：

依據 O-RAN Security Test Specification [12] 之第 9.4.1 小節。

(b) 測試目的：

確認軟體物料清單(Software Bill of Materials, SBOM)有有效的數位簽章。

(c) 測試前提：

無。

(d) 測試佈局：

見圖 92。

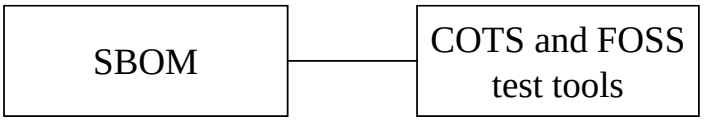


圖 90 軟體物料清單簽章測試示意圖

(e) 測試步驟：

(1) 確認軟體物料清單(SBOM)有軟體供應商公開金鑰(public key)或認證(certificate)的數位簽章。

(2) 當軟體物料清單(SBOM)採用軟體套件授權資料交換標準(Software Package Data Exchange, SPDX)格式時

i. YAML 不是一種標記語言(YAML Ain't a Markup Language, YAML)、資源描述格式(Resource Description Format, RDF)和標籤資料(tag data)的簽章需要與軟體套件授權資料交換標準(SPDX)檔案分離，例如 foo.spdx 之軟體物料清單(SBOM)的簽章為 foo.spdx.sig。

ii. 可延伸標示語言元(Extensible Markup Language, XML)的部分採用可延伸標示語言元簽章 2.0 版(XML Signature 2.0)。

iii. 爪哇腳本物件表示法(JavaScript object notation, JSON)的部分採用爪哇腳本物件表示法網頁簽章(JSON Web Signature, JWS)與爪哇腳本物件表示法簽章格式(JSON Signature Format, JSF)。

(3) 當軟體物料清單(SBOM)採用 CycloneDX 格式時

i. 可延伸標示語言元(XML)的部分採用可延伸標示語言元簽章 2.0 版(XML Signature 2.0)。

ii. 爪哇腳本物件表示法(JSON)的部分採用爪哇腳本物件表示法網頁簽章(JSON Web Signature, JWS)與爪哇腳本物件表示法簽章格式(JSON Signature Format, JSF)。

(4) 當軟體物料清單(SBOM)採用軟體識別(Software Identification, SWID)格式時

i. 可延伸標示語言元(XML)的部分採用可延伸標示語言元簽章 2.0 版(XML Signature 2.0) 。

(f) 測試結果：

(1) 根據步驟(1)至(4)，確認軟體物料清單(SBOM)有軟體供應商提供的有效數位簽章。

6.2.5.3 軟體物料清單資料欄位

(a) 測試依據：

依據 O-RAN Security Test Specification [12] 之第 9.4.2 小節。

(b) 測試目的：

確認軟體物料清單(Software Bill of Materials, SBOM)包含必要欄位。

(c) 測試前提：

無。

(d) 測試佈局：

見圖 93。

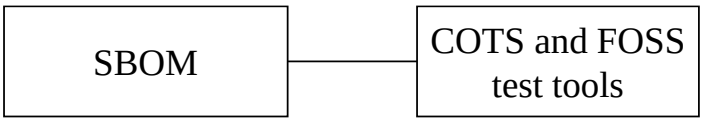


圖 91 軟體物料清單資料欄位測試示意圖

(e) 測試步驟：

(1) 確認軟體物料清單包含下列必要欄位。

(2) 當軟體物料清單(SBOM)採用軟體套件授權資料交換標準(Software Package Data Exchange, SPDX)格式時

(3) 當軟體物料清單(SBOM)採用 CycloneDX 格式時

(4) 當軟體物料清單(SBOM)採用軟體識別(Software Identification, SWID)格式時

表 6 軟體物料清單(SBOM)採用軟體套件授權資料交換標準(SPDX)格式的必要欄位

美國國家電信資訊管理局(NTIA)欄位	美國國家電信資訊管理局(NTIA)描述	軟體套件授權資料交換標準 2.2.1 版欄位
供應者名	建立、定義和組件標識的實體名稱	套裝軟體供應商
組件名稱	原始供應商分配定義的軟體單元名稱	套裝軟體名稱
組件版本	套裝軟體供應商用來區別版本修改的識別符	套裝軟體版本
其他唯一識別符	用相關數據庫識別與查詢組件或服務的其他唯一識別符	軟體套件授權資料交換標準識別符(SPDX Identifier, SPDXID)
相依關係	用於識別軟體 Y 包含上層組件 X 的關聯性	關聯: 包含(CONTAINS)
軟體物料清單資料作者	建立軟體物料清單的實體名稱	產生者
時間戳記	建立軟體物料清單的日期和時間記錄	建立

表 7 軟體物料清單(SBOM)採用 CycloneDX 格式的必要欄位

美國國家電信資訊管理局(NTIA)欄位	美國國家電信資訊管理局(NTIA)描述	CycloneDX 欄位
供應者名	建立、定義和組件標識的實體名稱	出版商
組件名稱	原始供應商分配定義的軟體單元名稱	名稱
組件版本	套裝軟體供應商用來區別版本修改的識別符	版本
其他唯一識別符	用相關數據庫識別與查詢組件或服務的其他唯一識別符	bom/serialNumber 與 component/bom-ref
相依關係	用於識別軟體 Y 包含上層組件 X 的關聯性	巢套組件/次組件與相依圖
軟體物料清單資料作者	建立軟體物料清單的實體名稱	bom-descriptor:metadata/ manufacture/contact
時間戳記	建立軟體物料清單的日期和時間記錄	時間戳記

表 8 軟體物料清單(SBOM)採用軟體識別(SWID)格式的必要欄位

美國國家電信資訊管理局(NTIA)欄位	美國國家電信資訊管理局(NTIA)描述	軟體識別(SWID)標籤
供應者名	建立、定義和組件標識的實體名稱	<Entity> @role (softwareCreator/publisher), @name
組件名稱	原始供應商分配定義的軟體單元名稱	<softwareIdentity> @name
組件版本	套裝軟體供應商用來區別版本修改的識別符	<softwareIdentity> @version
其他唯一識別符	用相關數據庫識別與查詢組件或服務的其他唯一識別符	<softwareIdentity> @tagID
相依關係	用於識別軟體 Y 包含上層組件 X 的關聯性	<Link> @rel, @href
軟體物料清單資料作者	建立軟體物料清單的實體名稱	<Entity> @role (tagCreator), @name
時間戳記	建立軟體物料清單的日期和時間記錄	-

(f) 測試結果：

(1) 根據步驟(1)至(4)，確認軟體物料清單包含必要欄位。

6.2.5.4 軟體映像簽章

(a) 測試依據：

依據 O-RAN Security Test Specification [12] 之第 9.5.1 和 15.2 小節。

(b) 測試目的：

確認軟體映像檔案有有效的數位簽章。

(c) 測試前提：

無。

(d) 測試佈局：

見圖 92。

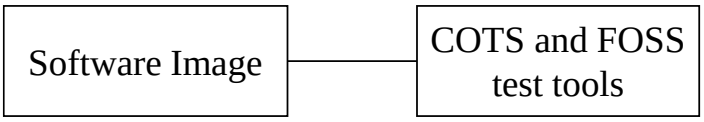


圖 92 軟體映像簽章測試示意圖

(e) 測試步驟：

(1) 採用人工方式或透過簽章軟體(如 Sigstore)對軟體映像檔案進行數位簽章。

(2) 確認產生金鑰配對：建議採用 prime256v1 短鑰配對(ephemeral key pair)。

(3) 確認私密金鑰(private key)與公開金鑰(public key)於使用後應立即刪除。

(4) 確認請求數位簽章認證，建議採用短壽命的認證(short-lived certificate)。

(5) 確認軟體映像檔案的雜湊(hash)與簽章(signing)採用 SHA256 或更強的演算法。

(f) 測試結果：

(1) 根據步驟(1)至(5)，確認軟體物料清單(SBOM)有軟體供應商提供的有效數位簽章。

6.2.5.5 軟體簽章驗證

(a) 測試依據：

依據 O-RAN Security Test Specification [12] 之第 9.5.2 和 15.2 小節。

(b) 測試目的：

確認軟體映像檔案載入時，有確認有效的數位簽章。

(c) 測試前提：

無。

(d) 測試佈局：

見圖 93。

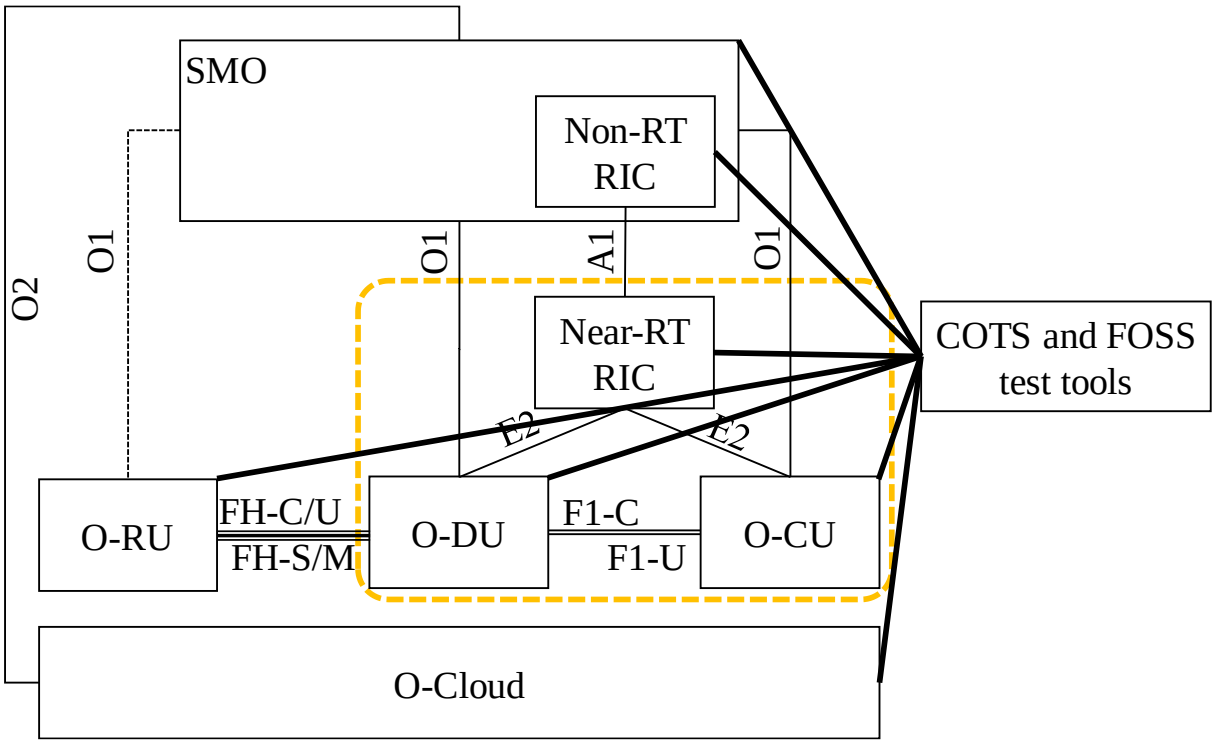


圖 93 軟體簽章驗證測試示意圖

(e) 測試步驟：

(1) 採用人工方式或透過簽章軟體(如 Sigstore)對軟體映像檔案進行數位簽章。

(2) 確認軟體映像檔案載入時，有確認有效的數位簽章。

(f) 測試結果：

(1) 根據步驟(1)至(2)，確認軟體映像檔案載入時，有確認有效的數位簽章。

6.2.5.6 O1 介面網路組態存取控制模型驗證

(a) 測試依據：

依據 O-RAN Security Test Specification [12] 之第 17.2 小節。

(b) 測試目的：

確認 O1 介面以角色為基礎的網路組態存取控制模型(Network Configuration Access Control Model, NACM) 做網路組態(NETCONF)的安全設定。

(c) 測試前提：

(1) 待測物已經載入憑證機構(Certificate Authorities, CAs)之憑證。

(2) 測試人員能夠使用用戶端根憑證(Client's root CA)透過 O1 介面進行網路組態(NETCONF)的安全設定測試。

(3) 已經透過傳送層安全協定(TLS)設好用戶端對網路組態(Client-to-NETCONF)的用戶名稱映射。

(d) 測試佈局：

見圖 94。

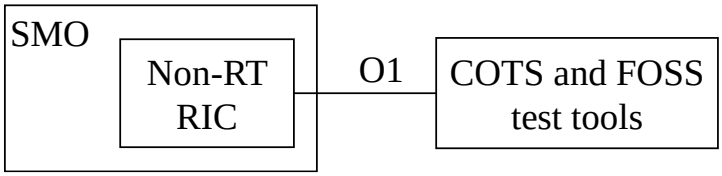


圖 94 O1 介面網路組態存取控制模型驗證測試示意圖

(e) 測試步驟：

(1) 使用 O1_nacm_managementf 群組之用戶帳號透過 O1 介面以 TLSv1.2 或 TLSv1.3 模式建立安全連線。

(2) 確認成功使用正確網路組態(NETCONF)的用戶帳號建立連線。

(3) 確認全域網路組態存取控制模型之強制控制設定(global NACM enforcement control setting)如下

i. enable-nacm = true

ii. read-default = permit

iii. write-default = deny

iv. exec-default = deny

v. enable-external-groups = true

(4) 確認預設之網路組態存取控制模型規則集合(NACM rule sets)如下

i. O1_nacm_management

ii. O1_user_management

iii. O1_network_management

iv. O1_network_monitoring

v. O1_software_management

(5) 關閉 O1 介面之安全連線。

(f) 測試結果：

(1) 根據步驟(3)至(4)，確認 O1 介面的網路組態存取控制模型(NACM)之網路組態(NETCONF)的安全設定設定正確。

附錄 A

(參考)

Open RAN 資安測試案例

依據無線接取網路聯盟(O-RAN Alliance)之安全工作小組(SWG)及測試與整合焦點小組(TIFG)所訂之資安測試標準(Security Test Specification)規格文件[15][20]所規定之資安測試工具與資安測試案例如下表所示。

表 9 Open RAN 資安測試案例[15]

案例編號	測試案例	案例描述
7.1.1	無線電資源控制(RRC)信令完整性保護	驗證 O-CU 傳送至用戶設備的 RRC 信令受到完整性保護。
7.1.2	用戶平面數據資料完整性保護	驗證 O-CU 傳送至用戶設備的用戶數據資料受到完整性保護。
7.1.3	無線電資源控制(RRC)信令完整性檢查失敗	驗證 O-CU 有正確處置收到完整性檢查失敗的 RRC 信令。
7.1.4	用戶平面完整性檢查失敗	驗證 O-CU 有正確處置收到完整性檢查失敗的用戶平面資料。
7.1.5	無線電資源控制信令加密	驗證 O-CU 傳送至用戶設備的 RRC 信令受到機密性保護。
7.1.6	用戶平面數據資料加密	驗證 O-CU 傳送至用戶設備的用戶平面資料受到機密性保護。
7.1.7	用戶平面數據資料重播攻擊保護	驗證 O-CU 接收到的用戶平面資料受到重播攻擊保護。
7.1.8	無線電資源控制(RRC)信令重播攻擊保護	驗證 O-CU 接收到的 RRC 制信令受到重播攻擊保護。
7.1.9	根據連結管理功能	驗證用戶平面資料依據 SMF 安全策略受到機密

案例編號	測試案例	案例描述
	(SMF)發送的安全策略對用戶平面資料進行加密	性保護。
7.1.10	基於連結管理功能(SMF)傳送的安全策略對用戶平面資料進行完整性保護	驗證用戶平面資料依據 SMF 的安全策略受到完整性保護。
7.1.11	O-RAN 集中單元接取層加密和完整性演算法優先順序	驗證 O-CU 接取層加密和完整性演算法優先順序設定運作正常。
7.1.12	6.1.3.2 O-RAN 集中單元金鑰更新-重複使用資料無線電承載識別碼	
7.1.13	6.1.4.1 防範 Xn 介面交遞中的降階攻擊	驗證當發生 Xn 交遞時預防降階攻擊的檢查機制。
7.1.14	6.1.4.2 在 Xn 介面交遞中接取層安全演算法選擇	驗證當發生 Xn 交遞時接取層安全演算法選擇機制。
7.1.15	控制平面資料在 N2/Xn/F1 介面的機密性保護	驗證 N2/Xn/F1 介面控制平面資料符合網際網路安全協定 (IPsec) 加密和認證達到機密性保護
7.1.16	控制平面資料在 N2/Xn/F1 介面的完整性保護	驗證 N2/Xn/F1 介面控制平面資料符合網際網路安全協定 (IPsec) 加密和認證達到完整性保護。
7.1.17	O-RAN 集中單元金鑰金鑰更新	驗證次節點之 O-RAN 基地臺當達到封包資料匯聚通訊協定計數環繞時次節點金鑰(K_{SN})更新功能運作正常。 驗證當達到重複使用資料無線電承載識別碼時，次節點金鑰 (K_{SN}) 更新功能運作正常。
7.2.1	開放前傳介面 S-Plane 阻斷服務測試	驗證當 O-RAN 分散單元的開放前傳介面 S-Plane 遭受阻斷服攻擊時，O-RAN 分散單元的性能不

案例編號	測試案例	案例描述
		會受到影響。
7.2.2	開放前傳介面 C-Plane 阻斷服務測試	驗證當 O-DU 的開放前傳介面 C-Plane 遭受阻斷服務攻擊時，O-DU 的性能不會受到影響。
7.2.3	A1 介面阻斷服務測試	驗證當 Near-RT RIC 的 A1 介面遭受非預期訊號攻擊時，Near-RT RIC 的性能不會受到影響。
7.2.4	開放前傳介面 S-Plane 模糊測試	驗證當 O-DU 的開放前傳介面 S-Plane 遭受非預期訊號攻擊時，O-DU 的性能不會受到影響。
7.2.5	開放前傳介面 C-Plane 模糊測試	驗證當 O-DU 的開放前傳介面 C-Plane 遭受非預期訊號攻擊時，O-DU 的性能不會受到影響。
7.2.6	A1 介面模糊測試	驗證當 Near-RT RIC 的 A1 介面遭受非預期訊號攻擊時，Near-RT RIC 的性能不會受到影響。
7.2.7	A1 介面已知弱點掃描	Near-RT RIC 的 A1 介面不應存在重大風險已知弱點漏洞，驗證是否存在中高風險已知弱點。
7.3	O-Cloud 虛擬化安全	確認當 O-RAN 遭受資源耗盡的旁通道阻斷服務攻擊 (noisy neighbor DoS attack) 時，O-Cloud 的性能不會受到影響。
STC-6-001	安全外殼協定(SSH)的伺服器與用戶端	安全外殼協定(Secure Shell, SSH)需要使用足夠強大加密協定套件。
STC-6-002	傳送層安全協定(TLS)	支援適當配置的傳送層安全協定(Transport Layer Security protocol, TLS)1.2 版或 1.3 版。
STC-6-003	資料包傳送層安全協定(DTLS)	支援適當配置的資料包傳送層安全協定(Datagram Transport Layer Security protocol, DTLS)1.2 版。
STC-6-004	網際網路安全協定(IPSec)	驗證網際網路安全協定(Internet Protocol Security, IPSec)是否正確設定通信安全協議。
STC-6-005	OAuth 2.0	驗證 OAuth 2.0 的認證機制。
STC-7-7.2-001	網路服務列舉(Service	不允許未註冊的網路服務。

案例編號	測試案例	案例描述
	Enumeration)	
STC-7-7.3-001	暴力破解(Brute Forcing)	不允許未經授權存取管理平面。
STC-7-7.3-002	未經授權的密碼重置(Unauthorized Password Reset)	確認沒有任何未經授權規避、停用或重置管理員(Admin)密碼的機制。
STC-7-7.3-003	強制密碼政策(Password Policy Enforcement)	確認會強制執行密碼政策(Password Policy)。
STC-7-7.4	模糊測試(Fuzzing)	測試 O-RAN 系統中使用之串流控制傳輸協定(Stream Control Transmission Protocol, SCTP)、網際網路協定(Internet protocol, IP)、傳輸控制協定(Transmission Control Protocol, TCP)、用戶資料元協定(User Datagram Protocol, UDP)、安全外殼協定模糊測試(SSH protocol)、超文件傳輸協定(Hypertext transfer protocol, HTTP)與超文件傳輸協定第 2 版(HTTP/2)、網路設定協定(NETCONF)、E1 應用協定(E1AP)、E2 應用協定(E2AP)、A1 協定、協同傳輸介面(Cooperative Transport Interface, CTI)、演進版通用公共無線電介面(evolved Common Public Radio Interface, eCPRI)以及精確時間協定(Precision Time Protocol, PTP)模糊測試的強健性。
STC-7-7.5-001	阻斷服務/資訊洪水(Denial of Service / Message Flooding	O-RAN 基地臺和主要介面需要具備足夠的強健性來抵抗分散式阻斷服務(Distributed Denial of Service, DDoS)攻擊。
STC-8-8.2-001	系統弱點掃描(System Vulnerability Scanning)	透果對 O-RAN 基地臺進行弱點掃描(Vulnerability Scanning)以確保 O-RAN 元件的作業系統(Operating System, OS)及應用程式(applications)無已知弱點。
STC-8-8.3	資料與資訊防護(Data and Information Protection)	N/A
STC-8-8.4	系統紀錄 (System logging)	N/A

案例編號	測試案例	案例描述
STC-9-9.2	開源軟體元件分析 (Open-Source Software Component Analysis)	N/A
STC-9-9.3	二元碼靜態分析 (Binary Static Analysis)	N/A
STC-9-9.4-001	軟體物料清單簽章 (SBOM Signature)	確認軟體物料清單 (SBOM) 有數位簽章保護。
STC-9-9.4-002	軟體物料清單資料欄位 (SBOM Data Fields)	驗證軟體物料清單 (SBOM) 包含必要資料欄位 (Data Fields)。
STC-9-9.5-001	軟體映像簽章 (Software Image Signing)	確認軟體映像簽章 (Software Image) 有數位簽章保護。
STC-9-9.5-002	軟體簽章驗證 (Software Signature Verification)	驗證軟體映像簽章 (Software Image) 的數位簽章有效性。
STC-10-10.2-001	機器學習資料毒害 (ML Data Poisoning)	N/A
STC-11.2-001	驗證者驗證 (Authenticator Validation)	確認 IEEE 802.1X-2020 Port-based Network Access Control 的驗證者驗證 (Authenticator Validation) 安全功能。
STC-11.2-002	申請者驗證 (Supplicant Validation)	確認 IEEE 802.1X-2020 Port-based Network Access Control 的申請者驗證 (Supplicant Validation) 安全功能。
STC-12	O-RU 資安測試	N/A
STC-13.2	Near-RT RIC 資安測試	確認 E2 介面受到網際網路安全協定(IPSec)保護。
STC-14.2	Non-RT RIC 資安測試	確認 A1 介面受到傳送層安全協定(TLS)保護。
STC-15.2	xApp 簽章與認證 (xApp Signing and	確 xApp 軟體映像簽章 (Software Image) 有數位

案例編號	測試案例	案例描述
	Verification)	簽章保護。
STC-16.1	rApp 資安測試	N/A
STC-17-17.2-001	O1 介面網路組態存取控制模型驗證 (O1 Interface NACM Validation)	驗證 O1 介面以角色為基的網路組態存取控制模型(Network Configuration Access Control Model, NACM) 做網路組態(NETCONF)的安全設定。
STC-18.1	O-Cloud 資安測試	N/A
STC-19.1	VNF/CNF/PNF 資安測試	N/A

附錄 B

(參考)

議題風險評估

(a) 議題描述

網際網路安全協定 (IPsec) 功能未開啟或未實作 Xn 介面

(b) 議題無法修改原因

(1) 內網與機房基礎防護可以降低資安風險，故 Xn 介面、F1 介面、E2 介面、N2 介面或 N3 介面並未曝露

(2) O-CU 與 O-DU 並未實體拆分，故 F1 介面並未曝露

(3) Near-RT RIC 和 O-CU 與 O-DU 並未實體拆分，故 E2 介面並未曝露

(4) 多台 O-DU 連接單台 O-CU，故 O-CU 並未實作 Xn 介面

(c) 風險綜合評估結果

列舉風險均透過應對措施降低風險至極低程度，故此議題可視為合規

表 B.1 議題風險評估表

編號	風險項目	風險說明	影響範圍	影響說明	應對措施	減緩程度	可否接受風險
1	網際網路安全協定 (IPsec) 功能未開啟傳輸資料被竊取	傳輸時未加密，導致可能遭偷聽竊取	Near-RT RIC、O-CU、O-DU	傳輸資料洩漏	(1)已裝設防火牆 (2)機房實體隔離管制出入	極高 (極高/高/中/低/極低)	可* (可/不可)
2	未實作 Xn 介面安全	Xn 介面交遞中的降階攻擊	O-CU	傳輸資料洩漏	O-CU 未實作 Xn 介面	極高	可*
3							

注*： 應對措施已足以將風險降至極低程度

參考資料

(1) 3GPP TR 21.905-h10, “Vocabulary for 3GPP Specifications (Release 17)”
(2) 3GPP TS 23.501-i10, “System Architecture for the 5G System(5GS) (Release 17)”
(3) 3GPP TS 38.413-h40, “NG-RAN; NG Application Protocol (NGAP) (Release 16)”
(4) 3GPP TS 29.281-h40, “General Packet Radio System (GPRS)Tunnelling Protocol User Plane (GTPv1-U) (Release 17)”
(5) 3GPP TS 38.423-h40, “NG-RAN; Xn Application Protocol (XnAP) (Release 16)”
(6) 3GPP TS 38.473-h30, “NG-RAN; F1 Application Protocol(F1AP) (Release 16)”
(7) 3GPP TS 38.463-h00, “NG-RAN; E1 Application Protocol(E1AP) (Release 16)”
(8) RAN WG3, “O-RAN E2 Application Protocol (E2AP) 3.0”
(9) RAN WG2, “O-RAN A1 interface: Application Protocol 4.0”
(10) RAN WG10, “O-RAN Operations and Maintenance Interface Specification 9.0”
(11) RAN WG6, “O-RAN O2 Interface General Aspects and Principles 3.0”
(12) RAN WG4, “O-RAN Control, User and Synchronization Plane Specification 11.0”

版本修改紀錄

版本	時間	摘要
v1.0	2023/07/20	出版

地　址・台北市中正區北平東路30-2號6樓
電　話・+886-2-23567698
Email・secretariat@taics.org.tw
www.taics.org.tw