



TAICS TS-0035 v2.0 : 2022

5G 基地臺資安測試規範 v2

Cybersecurity test specification for gNodeBs v2

2022/10/20

社團法人台灣資通產業標準協會
Taiwan Association of Information and Communication Standards

5G 基地臺資安測試規範 v2

Cybersecurity test specification for gNodeBs v2

出版日期: 2022/10/20

終審日期: 2022/09/23

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、王聖銘

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、台灣是德科技股份有限公司、台灣檢驗科技股份有限公司、安華聯網科技股份有限公司、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、國立陽明交通大學、趨勢科技股份有限公司、中興保全科技股份有限公司、亞太電信股份有限公司、友達光電股份有限公司、數位身分股份有限公司、華電聯網股份有限公司、和碩聯合科技股份有限公司

本計畫專案參與廠商(法人)名單為(以中文名稱順序排列)：

雲達科技股份有限公司、墩城科技有限公司、瑞擎數位股份有限公司、韋萊韜悅保險經紀人股份有限公司、智慧光科技股份有限公司、金融資安資訊分享與分析中心、凸版蓋特資訊股份有限公司

本規範由數位發展部支持研究制定。

目錄

誌謝.....	1
目錄.....	2
前言.....	3
引言.....	4
1. 適用範圍.....	6
2. 引用標準.....	7
3. 用語及定義.....	8
4. 5G 資安風險分析與需求.....	15
5. 資安測試分類與測試環境.....	17
5.1 行動通訊安全.....	18
5.2 系統與應用服務安全.....	19
5.3 測試環境.....	21
6. 資安測試規範.....	24
6.1 行動通訊安全.....	24
6.2 系統與應用服務安全.....	82
附錄 A (參考) gNB 資安測試標準對應表.....	113
附錄 B (參考) 議題風險評估表.....	117
參考資料.....	118
版本修改紀錄.....	120

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

依據歐盟與北約組織在 2019 年 5 月在 5G 安全會議所提出的「布拉格倡議 (Prague Proposals)」，可信任的 5G 網路軟硬體設備供應鏈管理，將是 5G 資安管理最重要的關鍵議題。因此，5G 電信事業不僅需要可信任的網路軟硬體設備供應鏈業者，更必須有能力驗證 5G 相關網路軟硬體設備的安全性才行。5G 資安可以從制度面、管理面和技術面三個層次闡述，但最重要的內涵就是要做到安全設計 (Security By Design)，也就是所有電信業者在進行 5G 網路建設之初，就必須納入資通安全防護機制。未來在營運時，也具備足夠的資安防護能量，真正做到確保 5G 網路的安全性，也可以進一步做到促進各種垂直應用場域及創新應用服務的發展。

臺灣在 5G 技術產業鏈中，除了手機晶片外，基地臺也是其中重要的發展項目，並藉以形成產業鏈。由於基地臺可能部署在非受控之暴露環境，同時也是核心網路的主要入口，因此極可能遭受設備實體入侵與後端傳輸網路入侵等威脅。然而，目前臺灣基地臺製造廠商大多僅具備 5G 互通性自主測試能量，尚未建構進一步自主資安的檢測能量。若政府於產業政策發展上能夠協助臺灣廠商在開發階段即早發現資安相關問題，不僅可大幅降低於入庫檢測時的資安修補成本，同時也可以提升產品的國際市場競爭力。

行政院科技會報辦公室於 2019 年 12 月 5 日發布行政院層級的「我國 5G 頻譜政策與專網發展」政策，5G 頻譜釋照將分階段逐步進行，且國家通訊委員會公告之「第五代行動通信系統資通安全維護計畫參考框架」，其技術面參考了第三代合作夥伴計畫 (3GPP) 國際資安標準規範與美國國家標準技術局 (National Institute of Standards and Technology, NIST) 的資安構架 (Cybersecurity Framework) 的規範，而管理與制度面參考了歐盟與北約組織的布拉格倡議以及歐盟 5G 網路安全風險評估報告。

有鑑於 5G 多元應用型態於國內佈時需要依賴 5G 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，資策會資安所團隊引用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) 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-0035 5G 基地臺資安測試規範」(以下簡稱本測試規範)，參考「3GPP TS 33.511 Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class」[1]、「3GPP TS 33.513 5G Security Assurance Specification (SCAS); User Plane Function (UPF)」[2]、「3GPP TS 33.117 Catalogue of general security assurance requirements」[3]、「3GPP TS 33.210 3G security; Network Domain Security (NDS); IP network layer security」[4]、「3GPP TS 33.310 Network Domain Security (NDS); Authentication Framework (AF)」[5]、「3GPP TS 33.501 Security architecture and procedures for 5G system」[6]、「3GPP TR 33.926 Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes」[7] 以及「3GPP TS 38.331 NR; Radio Resource Control (RRC) protocol specification」[8]，訂定 5G 基地臺之資安測試細節。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。

本版本(v2.0)之修正與勘誤，主要是根據 3GPP TS 33.117 與 TS 33.511 於 2021 年公布之最新版本內容有所更新，及實際資安之測試結果回饋。前後版本之條文對照，可以參考本規範之版本修改紀錄表。

1. 適用範圍

本測試規範規定 5G 獨立網組 (Standalone, SA) 架構下基地臺之資安測試實施要求。適用範圍包括圖 1 之紅框標註部分。5G 獨立組網(Standalone, SA)引用第三代合作夥伴計畫(3GPP)所定義之架構(9)，即由用戶設備(User Equipment, UE)、5G 基地臺(gNodeB, gNB) 及 5G 核心網路 (5G Core Network, 5GC) 所組成，如下圖 1 所示。

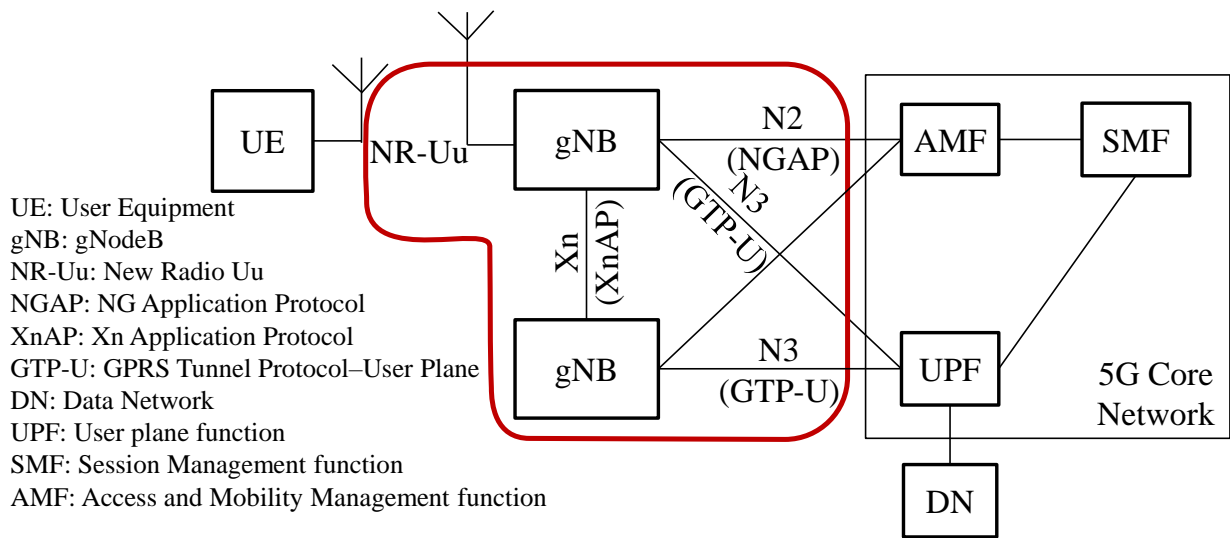


圖 1 適用範圍示意圖

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。下列引用標準適用最新版(包括補充增修)。

- [1] 3GPP TS 33.511-h10 Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class (Release 17)
(https://www.3gpp.org/ftp/Specs/archive/33_series/33.511/33511-h10.zip)
- [2] 3GPP TS 33.513-h00 5G Security Assurance Specification (SCAS); User Plane Function (UPF) (Release 17) (https://www.3gpp.org/ftp/Specs/archive/33_series/33.513/33513-h00.zip)
- [3] 3GPP TS 33.117-h00 Catalogue of general security assurance requirements (Release 17) (https://www.3gpp.org/ftp/Specs/archive/33_series/33.117/33117-h00.zip)
- [4] 3GPP TS 33.210-h00 3G security; Network Domain Security (NDS); IP network layer security (Release 17) (https://www.3gpp.org/ftp/Specs/archive/33_series/33.210/33210-h00.zip)
- [5] 3GPP TS 33.310-h20 Network Domain Security (NDS); Authentication Framework (AF) (Release 17) (https://www.3gpp.org/ftp/Specs/archive/33_series/33.310/33310-h20.zip)
- [6] 3GPP TS 33.501-h60 Security architecture and procedures for 5G system (Release 17) (https://www.3gpp.org/ftp/Specs/archive/33_series/33.501/33501-h60.zip)
- [7] 3GPP TR 33.926-h40 Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes (Release 17)
(https://www.3gpp.org/ftp/Specs/archive/33_series/33.926/33926-h40.zip)
- [8] 3GPP TS 38.331-h00 NR; Radio Resource Control (RRC) protocol specification (Release 17) (https://www.3gpp.org/ftp/Specs/archive/38_series/38.331/38331-h00.zip)

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 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 (10)，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。

3.3 gNB/gNodeB (Next generation NodeB)

gNB 或 gNodeB 乃指 3GPP 5G NR 系統架構中之 5G 基地臺，是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 (Macro 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(13)則用來提高基地臺的部署密度，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。

3.4 5GC (5G core network)

5GC 乃指 3GPP 5G NR 系統架構中之 5G 核心網路(9)，其透過控制平面 (Control plane) 與用戶平面 (User plane) 分離技術實現以服務為基礎 (Service based architecture, SBA) 之網路虛擬化 (Network virtualization) 架構。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 gNB。

3.5 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份驗證、非存取層 (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、用戶設備移動換手管理以及合法監聽 (Lawful interception, LI) 等功能(9)。

3.6 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(9)。

3.7 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(9)。

3.8 資料網路 (Data network, DN)

是一個將 5G 核心網路中用戶設備 (UE) 的傳輸資料到網際網路的資料交換網路節點，其包含電路交換 (circuit switch) 和租用線路 (leased line) 及分封交換網路 (packet switching network, PSN) 等網路設備。

3.9 非存取層 (Non access stratum, NAS)

非存取層為用戶設備 (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。

3.10 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[8]，主要提供非存取層 (NAS) 系統資訊廣播；建立、維護和釋放用戶設備 (UE) 與 gNB 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 gNB；服務品質 (QoS) 管理功能；非存取層 (NAS) 消息的傳輸等。

3.11 封包資料匯聚通訊協定 (Packet data convergence protocol, PDCP)

主要負責 IP 包頭壓縮與解壓縮，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，數據加密為可選功能，其中用戶平面的數據包含應用層信令，如 SIP，RTCP 等。

3.12 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 gNB 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 gNB 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。

3.13 下一代應用協定 (NG application protocol, NGAP)

為 gNB 和存取與移動管理功能 (AMF) 間處理下一代介面 (NG Interface) 之相關信令與程序 (14)，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、用戶設備移動換手管理以及轉送上下行鏈路之非存取層 (NAS) 信令。

3.14 Xn 應用協定 (Xn application protocol, XnAP)

為兩台 gNB 間處理 Xn 介面之相關信令與程序，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管理等(15)。

3.15 通用封包無線服務隧道協定-用戶平面 (GPRS tunnel protocol- user plane, GTP-U)

一個以 IP 為基礎的簡單穿隧協定(16)，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)。

3.16 NG-RAN/NR-Uu 介面 (Next generation radio access network, NG-RAN/NR-Uu Interface)

為用戶設備 (UE) 和 gNB 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(17)。

3.17 模糊測試工具 (Fuzz testing tool)

是一種軟體測試技術工具，可以被用作白盒，灰盒或黑箱測試。模糊測試工具主要分為兩類，變異測試 (mutation-based) 以及生成測試 (generation-based)。其核心思想是將自動或半自動生成的亂數據輸入到一個程式中，並監視程式異常以發現可能的程式錯誤。模糊測試常常用於檢測軟體或通訊系統的安全漏洞。因為模糊測試可以窮舉變異或生成測試的樣態，故本測試規範不定義模糊測試工具的量化標準。

3.18 gNB 模糊測試器 (gNB fuzz testing device)

為具備 gNB 網路元件功能並與待測 gNB 相同 Xn 介面連線之模擬裝置，能夠讓待測 gNB 透過 Xn 應用協定 (XnAP) 與 gNB 模糊測試裝置進行 gNB 間的資訊交換，並在檢測過程中能夠透過 Xn 介面對待測 gNB 發送非預期的 Xn 應用協定封包，用以驗證 gNB 的強健性。

3.19 UPF 模糊測試器 (UPF fuzz testing device)

為具備用戶平面功能 (UPF) 網路元件功能並與待測 gNB 相同 N3 介面連線之模擬裝置，能夠讓待測 gNB 透過 GTP-U 與存取與用戶平面功能裝置建立用戶設備 (UE) 資料通道，並在檢測過程中能夠透過 N3 介面對待測 gNB 發送非預期的通用封包無線服務隧道協定-用戶平面封包，用以驗證 gNB 的強健性。

3.20 AMF 模糊測試器 (AMF fuzz testing device)

為具備 AMF 並與待測 gNB 相同 N2 介面連線之模擬裝置，能夠讓待測 gNB 透過下一代應用協定 (NGAP) 與存取與移動管理功能模糊測試裝置進行註冊，並在檢測過程中能夠透過 N2 介面對待測 gNB 發送非預期的下一代應用協定封包，用以驗證 gNB 的強健性。

3.21 重播檢測裝置 (Replay testing device)

可以在 NG-RAN 介面擷取無線電資源控制 (RRC) 信令封包或用戶平面資料封包 [1]，並利用擷取的資料封包或分析擷取的封包 (如無線電資源控制 (RRC) 信令之無線電資源控制序號 (RRC SQN) 製作出相似的資料封包，透過 NG-RAN 介面對 gNB 發動重播攻擊。該裝置進一步在 NG-RAN 介面擷取無線電資源控制 (RRC) 信令封包或用戶平面資料封包，來確認是否 gNB 有任何回覆的封包，以確認 gNB 是否丟棄或忽略該重播攻擊的封包。

3.22 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份，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。

3.23 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(18)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。

3.24 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) 與隧道模式 (Tunnel mode) 兩種封包模式。

3.25 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) 與網際網路安全關聯與金鑰管理協定 (ISAKMP) 上的網路協定。該協定定義於 RFC 2409 標準規範(19)文件中。為了配合網際網路安全關聯與金鑰管理協定 (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。

3.26 營運管理與維護 (Operations, administration and maintenance, OA&M)

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)。

3.27 商用現成軟體 (Commercial-off-the-shelf, COTS)

是指事先寫好的一組應用程式軟體，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。

3.29 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. 5G 資安風險分析與需求

依據 3GPP TR 33.926 [6] 網路產品類別之威脅和關鍵資產的安全保證規範，從 5G 資安風險分析可以歸納出七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)、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 gNB 風險分析如下。

表 1 gNB 風險分析

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 介面威脅
	NR-Uu 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

5. 資安測試分類與測試環境

本測試規範參考第三代合作夥伴計畫所制定之「3GPP TS 33.511 Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class」[1]、「3GPP TS 33.513 5G Security Assurance Specification (SCAS); User Plane Function (UPF)」[2]與「3GPP TS 33.117 Catalogue of general security assurance requirement」[3]的資安需求 (security requirement)，針對 gNB 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件 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，僅提供 gNB 製造商、系統整合商與電信事業以及 5G 資安檢測實驗室等作為 gNB 相關產品「技術面」的檢測，「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」，同時應參考附件 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 33.511 Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class」[1] 之第 4.2.2 小節與「3GPP TS 33.513 5G Security Assurance Specification (SCAS); User Plane Function (UPF)」[2] 之第 4.2.2 小節，制定相對應之行動通訊安全測試項目。

表 2 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	無線電資源控制(RRC)與封包資料匯聚通訊協定(PDCP)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	用戶層資料保護機制	6.1.2.1 用戶設備和 gNB 間的用戶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 用戶設備和 gNB 間的用戶平面資料加密	NR-Uu 介面威脅 竊聽
		6.1.2.4 用戶設備與 gNB 間的用戶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	存取層安全演算法檢測	6.1.3.1 gNB 存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
		6.1.3.3 gNB 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
		6.1.3.4 gNB 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
		6.1.3.5 gNB 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	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 介面交遞中存取層安全演算法選擇	NR-Uu 介面威脅
6.1.5	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 N2 介面的完整性保護	N2 介面威脅 用戶通信期竄改
		6.1.5.5 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
		6.1.5.6 控制平面資料在 Xn 介面的完整性保護	Xn 介面威脅 用戶通信期竄改
6.1.6	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 介面的模糊測試(非必測項目)	Xn 介面威脅

5.2 系統與應用服務安全

本節參考「3GPP TS 33.511 5G Security Assurance Specification (SCAS); NR Node B (gNB)」[1] 之第 4.2.3 小節至第 4.4 小節與「3GPP TS 33.117 Catalogue of general security assurance requirement」[3] 之第 4.2.3 小節至第 4.4 小節，制定相對應之系統與應用服務安全測試項目。

表 3 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
6.2.3	身份鑑別與授權	6.2.3.1 禁止未經認證與授權使用系統各項功能	資提高特權-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 gNB 系統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 gNB 系統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
6.2.4	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 gNB 系統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錄功能轉移備存至外部系統	缺乏用戶活動記錄

	6.2.4.6 gNB 系統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

5.3 測試環境

本節描述本測試規範所需之測試環境與設備需求，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 4 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
		監聽 NG-RAN 介面的非存取層(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
	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 NG-RAN 介面完成連線註冊
		透過 NG-RAN 介面發送資料封包
		監聽 NG-RAN 介面的非存取層(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
		竄改 NG-RAN 介面的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
重播 NG-RAN 介面的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
		支援下一代應用協定(NGAP)和 Xn 應用協定(XnAP)介面
		支援 Xn 介面換手
		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
		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 GTP-U 介面
		監聽 GTP-U 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
		支援下一代應用協定(NGAP)介面
		監聽下一代應用協定(NGAP)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
--	-------------------------

6. 資安測試規範

6.1 行動通訊安全

6.1.1 無線電資源控制(RRC)與封包資料匯聚通訊協定(PDCP)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 [6] 之第 5.3.3 小節與 3GPP TR 33.926 [7] 之第 D.2.2.2 小節，並參考 3GPP TS 33.511 [1] 之第 4.2.2.1.1 小節。

(b) 測試目的：

驗證用戶設備和 gNB 間透過 NG-RAN 介面傳送的 RRC 信令受到完整性保護。

(c) 測試前提：

- (1) 用戶設備及 gNB 間可以進行完整性安全演算法設定。
- (2) 用戶設備、gNB 及 5GC 間可以成功建立 5G 連線。
- (3) 測試人員可擷取 NG-RAN 介面封包，並分析 RRC 封包之 PDCP 層的內容。

(d) 測試佈局：

見圖 2。

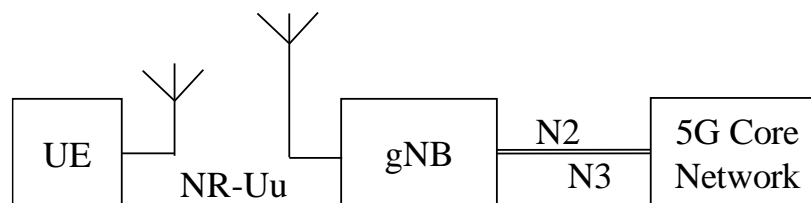


圖 2 RRC 信令完整性保護測試示意圖

(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 gNB 端設定 NIA1 完整性安全演算法為最優先選擇。
- (3) 開始擷取 NG-RAN 介面封包。
- (4) 確認 gNB 與 5GC 間建立 NGAP 連線，且用戶設備註冊上 5GC。
- (5) 停止擷取 NG-RAN 介面封包。
- (6) 透過 NG-RAN 介面封包，檢查用戶設備和 gNB 之 RRC 信令安全驗證程序。
- (7) 透過 NG-RAN 介面封包，在完成 RRC 信令安全驗證程序後，確認用戶設備和 gNB 間的 RRC 信令是否帶有完整性鑑別碼在對應的 PDCP 層的訊息。
- (8) 將 gNB 端設定 NIA2 完整性安全演算法為最優先選擇重複(2)~(7)測試。

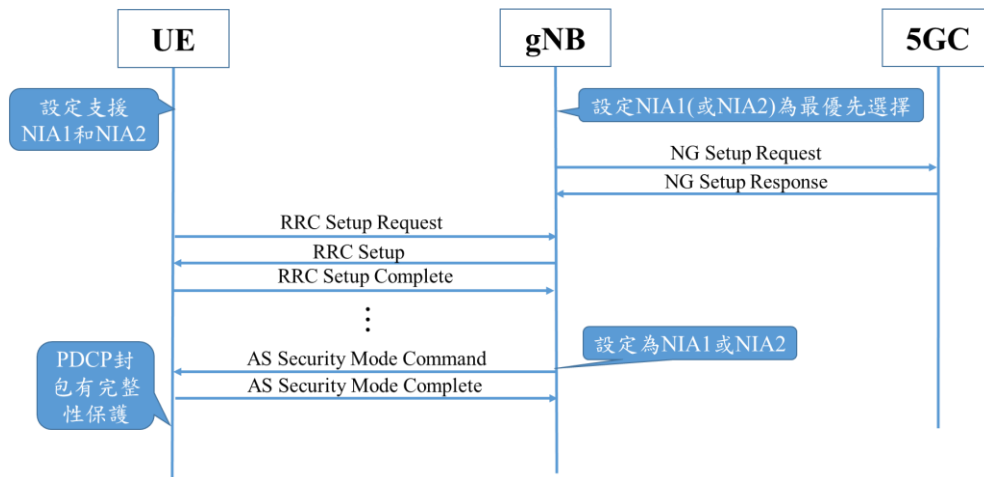


圖 3 RRC 信令的完整性保護測試流程圖

(f) 測試結果：

- (1) 根據步驟(6)，gNB 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(7)，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 gNB 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 [6] 之第 6.5.1 小節與 3GPP TR 33.926 [7] 之第 D.2.2.2 小節，並參考 3GPP TS 33.511 [1] 之第 4.2.2.1.4 小節。

(b) 測試目的：

驗證 gNB 有正確處置完整性檢查失敗的 RRC 信令。

(c) 測試前提：

- (1) 用戶設備及 gNB 間可以進行完整性安全演算法設定。
- (2) 用戶設備、gNB 及 5GC 間可以成功建立 5G 連線。
- (3) 用戶設備可以修改 RRC 信令對應之 PDCP 層的訊息完整性鑑別碼。
- (4) 測試人員可擷取 NG-RAN 介面封包，並分析 RRC 封包之 PDCP 層的內容。

(d) 測試佈局：

見圖 4。

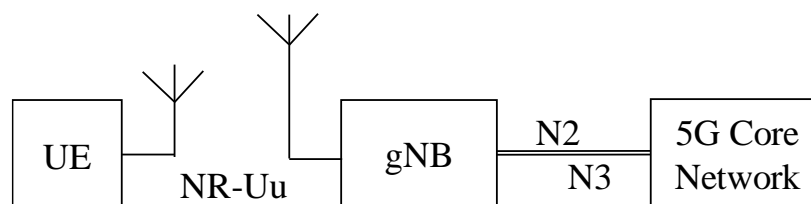


圖 4 RRC 信令完整性檢查失敗測試示意圖

(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 gNB 端設定 NIA1 完整性安全演算法為最優先選擇。
- (3) 開始擷取 NG-RAN 介面封包。
- (4) 確認 gNB 與 5GC 間建立 NGAP 連線，且用戶設備註冊。
- (5) 從 NG-RAN 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 gNB 的 RRC 信令封包。而選定的 RRC 信令之 PDCP 層的訊息帶有不合訊息完整性鑑別碼資訊或含錯誤的訊息完整性鑑別碼資訊。

- (6) 停止擷取 NR-RAN 介面封包。
- (7) 透過 NG-RAN 介面封包，確認 gNB 是否檢查完整性鑑別碼之正確性。
- (8) 將 gNB 端設定 NIA2 完整性安全演算法為最優先選擇重複(2)~(7)測試。

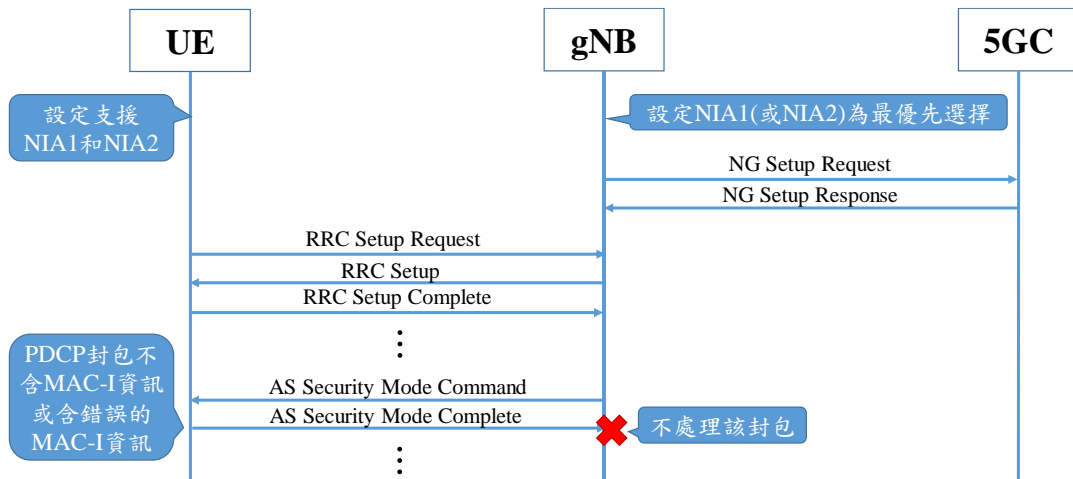


圖 5 RRC 信令完整性檢查失敗測試流程圖

(f) 測試結果：

- (1) 根據步驟(7)，gNB 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 AS Security Mode Complete 信令。

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 [6] 之第 5.3.2 小節與 3GPP TR 33.926 [7] 之第 D.2.2.1 小節，並參考 3GPP TS 33.511 [1] 之第 4.2.2.1.6 小節。

(b) 測試目的：

驗證透過 NG-RAN 介面傳送的 RRC 信令受到機密性保護。

(c) 測試前提：

- (1) 用戶設備及 gNB 間可以進行機密和完整性安全演算法設定。
- (2) 用戶設備、gNB 及 5GC 間可以成功建立 5G 連線。
- (3) 測試人員可擷取 NG-RAN 介面封包，並分析 RRC 封包之 PDCP 層的內容。

(d) 測試佈局：

見圖 6。

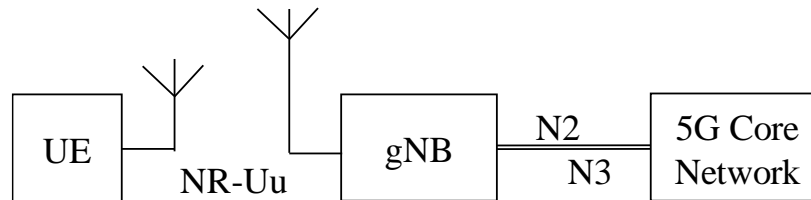


圖 6 RRC 信令加密測試示意圖

(e) 測試步驟：

- (1) 在用戶設備設定支援 NEA1、NEA2、NIA1、NIA2 機密和完整性安全演算法。
- (2) 在 gNB 端設定 NEA1、NIA1 機密和完整性安全演算法為最優先選擇。
- (3) 開始擷取 NG-RAN 介面封包。
- (4) 確認 gNB 與 5GC 間建立 NGAP 連線，且用戶設備註冊上 5GC。
- (5) 停止擷取 NG-RAN 介面封包。
- (6) 透過 NG-RAN 介面封包，檢查用戶設備和 gNB 之無線電資源控制信令安全驗證程序。
- (7) 透過 NG-RAN 介面封包，在完成 RRC 信令安全驗證程序後，確認用戶設備和 gNB 間的 RRC 信令是否在對應之 PDCP 層中的訊息進行加密。
- (8) 將 gNB 端設定 NEA2、NIA2 機密和完整性安全演算法為最優先選擇重複 (2)~(7) 測試。

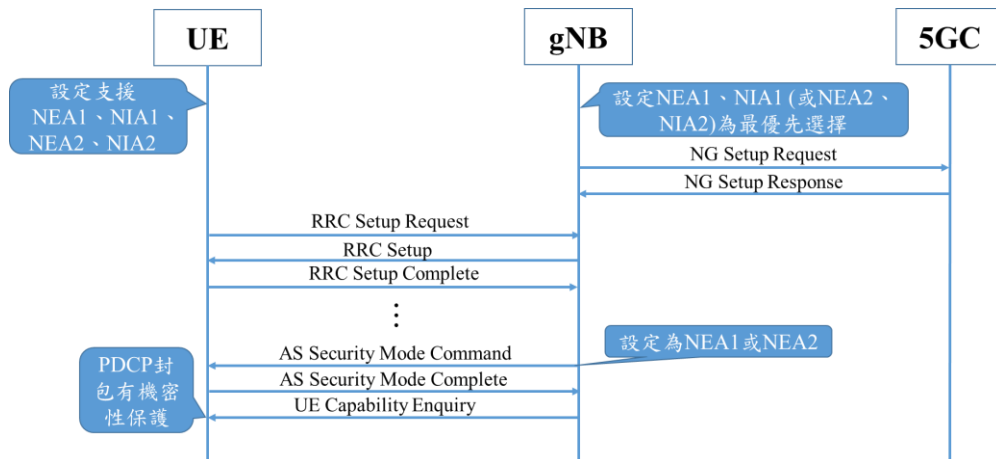


圖 7 RRC 信令加密測試流程圖

(f) 測試結果：

- (1) 根據步驟(6)，gNB 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(7)，PDCP 層中的訊息會被加密進行機密性保護。用戶設備和 gNB 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 [6] 之第 5.3.3 小節與 3GPP TR 33.926 [7] 之第 D.2.2.2 小節，並參考 3GPP TS 33.511 [1] 之第 4.2.2.1.9 小節。

(b) 測試目的：

驗證用戶設備和 gNB 間透過 NG-RAN 介面傳送的 RRC 制信令受到重播攻擊保護。

(c) 測試前提：

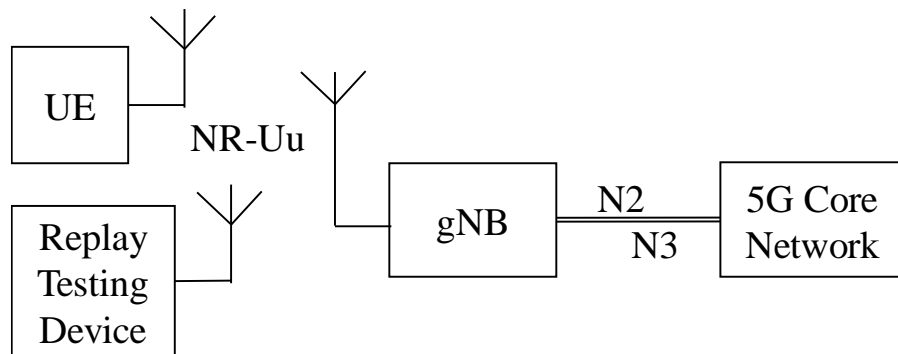
- (1) 用戶設備及 gNB 間可以進行機密和完整性安全演算法設定。
- (2) 用戶設備、gNB 及 5GC 間可以成功建立 5G 連線。

(3) 用戶設備可以重播特定 RRC 信令，其中重播信令的 PDCP 層以上的協定內容都要和原始信令一樣。

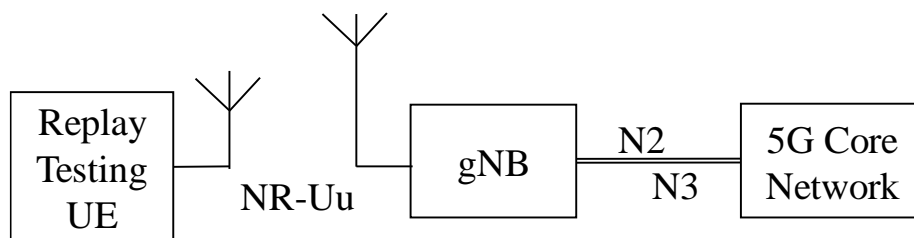
(4) 測試人員可擷取 NG-RAN 介面封包，並分析 RRC 封包之 PDCP 層的內容。

(d) 測試佈局：

見圖 8。



(a)透過重播裝置進行測試



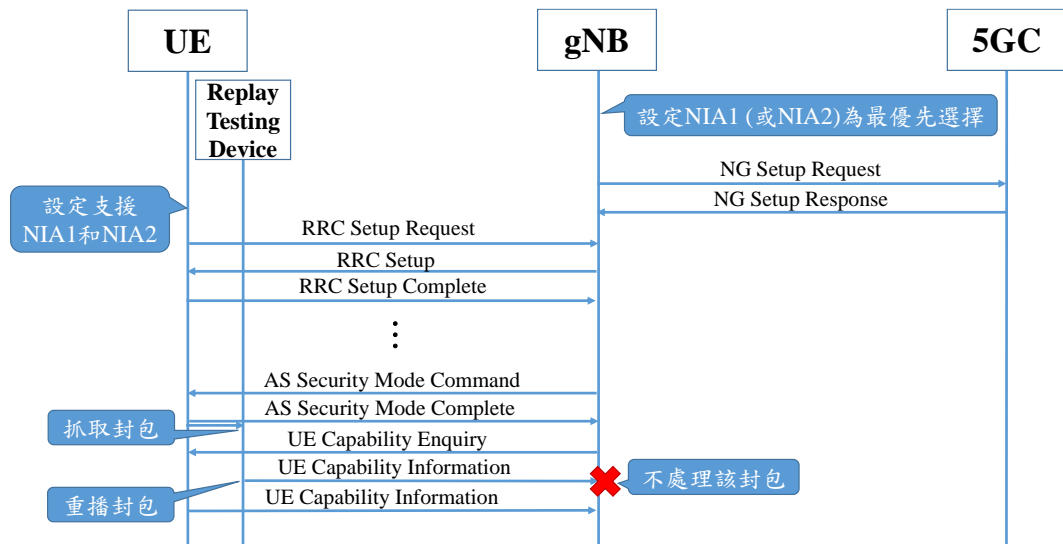
(b)透過具備重播功能的用戶設備進行測試

圖 8 RRC 信令重播攻擊保護測試示意圖

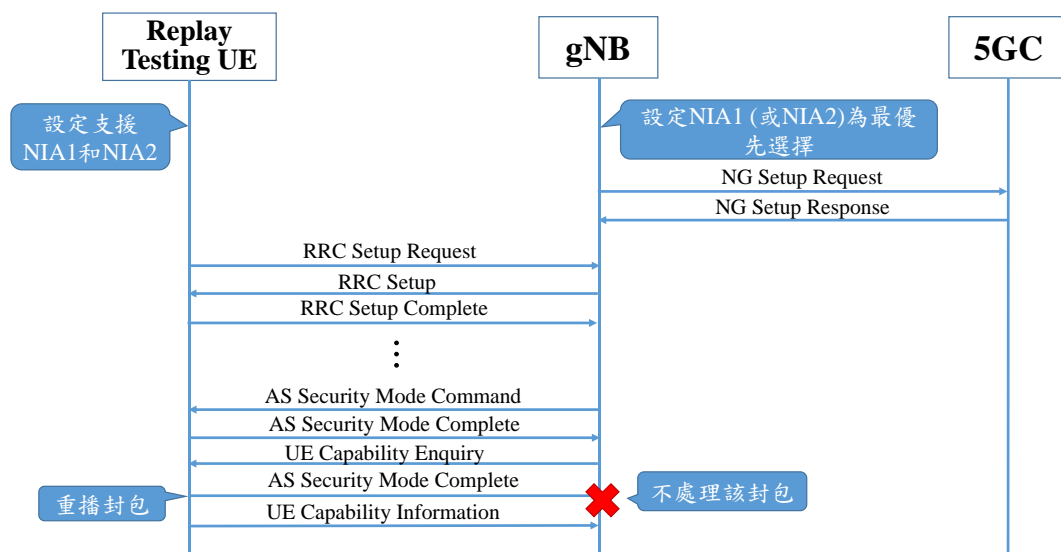
(e) 測試步驟：

- (1) 在用戶設備設定支援 NIA1 和 NIA2 完整性安全演算法
- (2) 在 gNB 端設定 NIA1 完整性安全演算法為最優先選擇。
- (3) 開始擷取下一代無線接取介面資料封包。
- (4) 確認 gNB 與 5GC 間建立 NGAP 連線，且用戶設備註冊 5G 網路。
- (5) 從 RN-RAN 介面資料封包確認用戶設備和 gNB 是否完成 RRC 信令安全驗證程序。

- (6) 從擷取的 NG-RAN 介面資料封包透過重播裝置選定特定 RRC 信令封包(如 AS Security Mode Complete)進行重播。而被重播的 RRC 信令的 PDCP 內容(含 PDCP 計數與訊息完整性鑑別碼)要和原始封包一樣。
- (7) 停止擷取 NG-RAN 介面資料封包。
- (8) 透過 NGAP 封包，確認 gNB 檢查重播的 RRC 信令在 PDCP 層帶有的 PDCP 計數是否重覆。
- (9) 將 gNB 端設定 NIA2 完整性安全演算法為最優先選擇重複(2)~(8)測試。



(a) 透過重播裝置進行測試



(b) 透過具備重播功能的用戶設備進行測試

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(8)，gNB 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 用戶層資料保護機制

6.1.2.1 用戶設備和基地臺間的用戶數據資料完整性保護

(a) 測試依據：

依據 3GPP TS 33.501 [6] 之第 5.3.3 小節與 3GPP TR 33.926 [7] 之第 D.2.2.4 小節，並參考 3GPP TS 33.511 [1] 之第 4.2.2.1.2 小節。

(b) 測試目的：

驗證透過 NG-RAN 介面傳送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 gNB 間可以進行完整性安全演算法設定。
- (2) 用戶設備、gNB 及 5GC 間可以成功建立 5G 連線。
- (3) SMF 要開啟用戶平面安全策略之用戶平面完整性保護指示。
- (4) 測試人員可擷取 NG-RAN 介面封包，並分析 RRC 與用戶平面封包之 PDCP 層的內容。

(d) 測試佈局：

見圖 10。

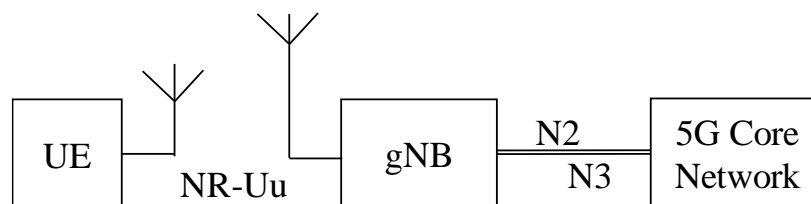


圖 10 用戶數據資料完整性保護測試示意圖

(e) 測試步驟：

- (1) 在用戶端設定支援 NIA1 和 NIA2 完整性安全演算法。
- (2) 在 gNB 端設定 NIA1 完整性安全演算法為最優先選擇。
- (3) 開始擷取 NG-RAN 介面封包。
- (4) 確認 gNB 與 5GC 間建立 NGAP 連線，且用戶設備註冊上 5GC 和傳送數據資料。
- (5) 停止擷取 NG-RAN 介面封包。
- (6) 透過 NG-RAN 介面封包，確認用戶設備和 gNB 完成 RRC 信令安全驗證程序後。
- (7) 透過 NG-RAN 介面封包，確認用戶設備和 gNB 透過 RRC Reconfiguration 完成用戶平面安全驗證程序。
- (8) 透過 NG-RAN 介面封包，確認用戶設備和 gNB 間的用戶平面封包所對應之 PDCP 層的訊息帶有完整性鑑別碼。
- (9) 將 gNB 端設定 NIA2 完整性安全演算法為最優先選擇重複(2)~(8)測試。

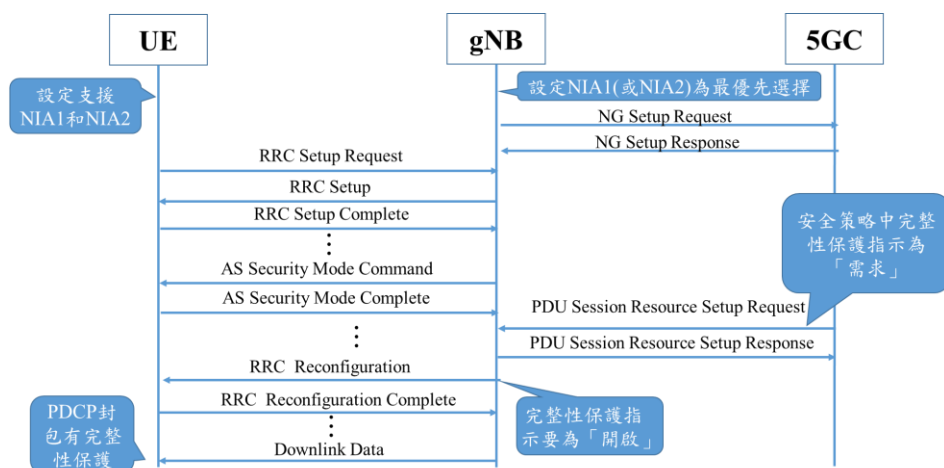


圖 11 用戶數據資料完整性保護測試流程圖

(f) 測試結果：

- (1) 根據步驟(7)，gNB 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(8)，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 gNB 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 [6] 之第 6.6.4 小節與 3GPP TR 33.926 [7] 之第 D.2.2.4 小節，並參考 3GPP TS 33.511 [1] 之第 4.2.2.1.5 小節。

(b) 測試目的：

驗證 gNB 有正確處置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 gNB 間可以進行完整性安全演算法設定。
- (2) 用戶設備、gNB 及 5GC 間可以成功建立 5G 連線。
- (3) SMF 要開啓用戶平面安全策略之用戶平面完整性保護指示。
- (4) 用戶設備可以修改用戶平面封包所對應的 PDCP 層訊息中的完整性鑑別碼。
- (5) 測試人員可擷取 NG-RAN 介面封包，並分析 RRC 與用戶平面封包之 PDCP 層的內容。

(d) 測試佈局：

見圖 12。

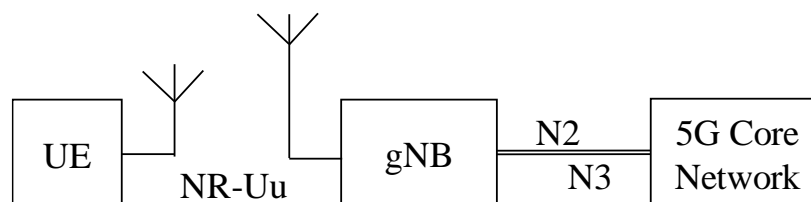


圖 12 用戶平面完整性檢查失敗測試示意圖

(e) 測試步驟：

- (1) 在用戶端設定支援 NIA1 和 NIA2 完整性安全演算法。
- (2) 在 gNB 端設定 NIA1 完整性安全演算法為最優先選擇。
- (3) 開始擷取 NG-RAN 介面封包。
- (4) 確認 gNB 與 5GC 間建立 NGAP 連線，且用戶設備註冊並傳送數據封包。
- (5) 用戶設備選擇特定發送給 gNB 的用戶平面封包。而選定的用戶平面封包帶有不含訊息完整性鑑別碼資訊或含錯誤的訊息完整性鑑別碼資訊在對應之 PDCP 層的訊息中。
- (6) 停止擷取 NG-RAN 介面封包。
- (7) 透過 NG-RAN 介面封包，確認 gNB 是否檢查完整性鑑別碼之正確性。
- (8) 將 gNB 端設定 NIA2 完整性安全演算法為最優先選擇重複(2)~(7)測試。

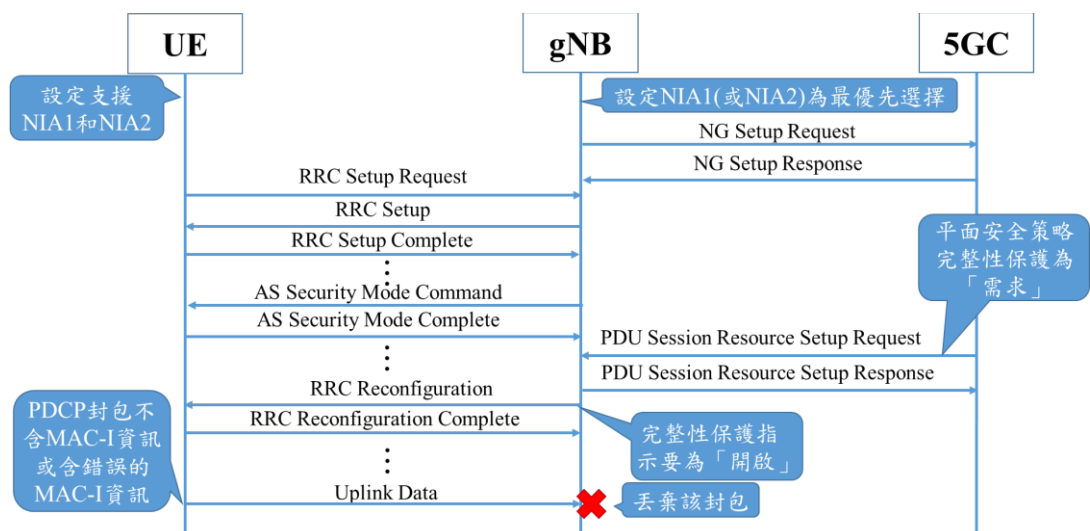


圖 13 用戶平面完整性檢查失敗測試流程圖

(f) 測試結果：

- (1) 根據步驟(7)，gNB 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 用戶設備和基地臺間的用戶平面資料加密

(a) 測試依據：

依據 3GPP TS 33.501 [6] 之第 5.3.2 小節與 3GPP TR 33.926 [7] 之第 D.2.2.3 小節，並參考 3GPP TS 33.511 [1] 之第 4.2.2.1.7 小節。

(b) 測試目的：

驗證透過 NG-RAN 介面傳送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 gNB 間可以進行機密和完整性安全演算法設定。
- (2) 用戶設備、gNB 及 5GC 間可以成功建立 5G 連線。
- (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) 測試人員可擷取 NG-RAN 介面封包，並分析 RRC 與用戶平面封包之 PDCP 層的內容。

(d) 測試佈局：

見圖 14。

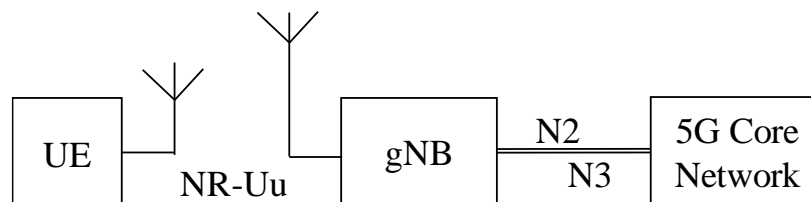


圖 14 用戶平面資料加密測試示意圖

(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 gNB 端設定 NEA1、NIA1 機密和完整性安全演算法為最優先選擇。
- (3) 開始擷取 NG-RAN 介面封包。
- (4) 確認 gNB 與 5GC 間建立 NGAP 連線，且用戶設備註冊和傳送數據封包。
- (5) 停止擷取 NG-RAN 介面封包。

- (6) 透過 NG-RAN 介面封包，確認用戶設備和 gNB 完成 RRC 信令安全驗證程序後。
- (7) 透過 NG-RAN 介面封包，確認用戶設備和 gNB 透過 RRC Reconfiguration 完成用戶平面安全驗證程序。
- (8) 透過 NG-RAN 介面封包，確認用戶設備和 gNB 間的用戶平面封包所對應之 PDCP 層的訊息被加密保護。
- (9) 將 gNB 端設定 NEA2、NIA2 機密和完整性安全演算法為最優先選擇重複 (2)~(8) 測試。

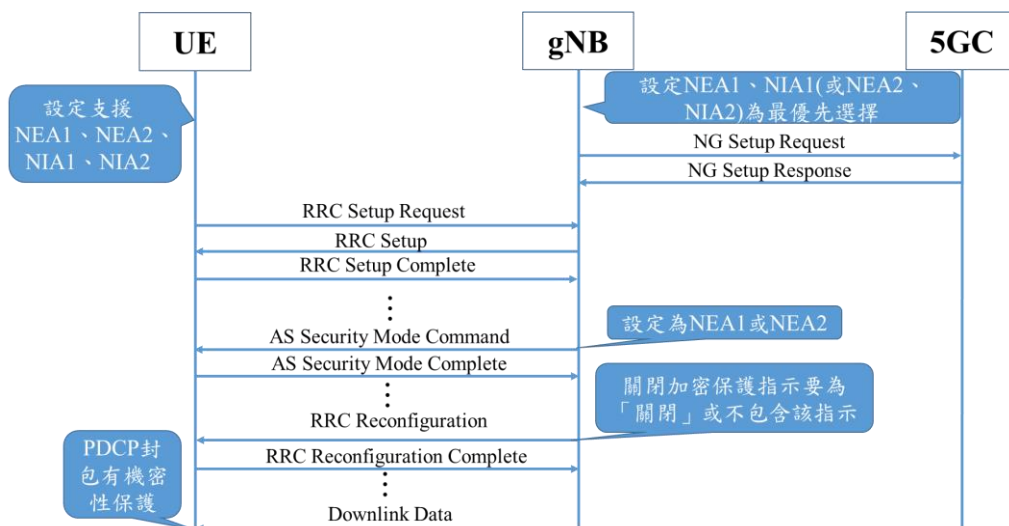


圖 15 用戶平面資料加密測試流程圖

(f) 測試結果：

- (1) 根據步驟(7)，gNB 傳送的 RRC Reconfiguration 中的關閉加密保護指示要為「關閉」或不包含該指示，並且用戶設備回應 RRC Reconfiguration Complete。
- (2) 根據步驟(8)，PDCP 層的訊息應受到加密保護。用戶設備和 gNB 因此進行用戶平面封包加密傳輸。

6.1.2.4 用戶設備與基地臺間的用戶數據資料重播攻擊保護

(a) 測試依據：

依據 3GPP TS 33.501 [6] 之第 5.3.3 小節與 3GPP TR 33.926 [7] 之第 D.2.2.4 小節，並參考 3GPP TS 33.511 [1] 之第 4.2.2.1.8 小節。

(b) 測試目的：

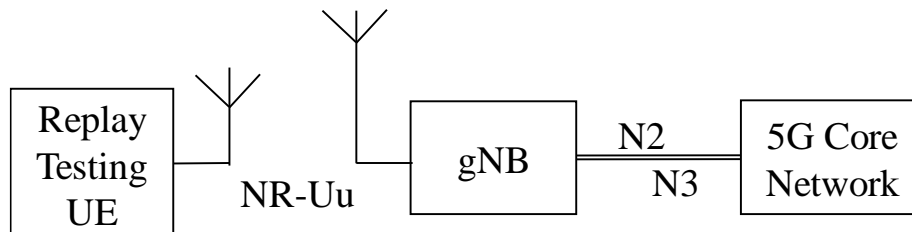
驗證用戶設備和 gNB 間透過 NG-RAN 介面傳送的用戶平面資料受到重播攻擊保護。

(c) 測試前提：

- (1) 用戶設備及 gNB 間可以進行機密和完整性安全演算法設定。
- (2) 用戶設備、gNB 及 5GC 間可以成功建立 5G 連線。
- (3) SMF 要開啟用戶平面安全策略之用戶平面完整性保護指示。
- (4) 測試人員可擷取 NG-RAN 介面封包，並分析 RRC 與用戶平面封包之 PDCP 層的內容。

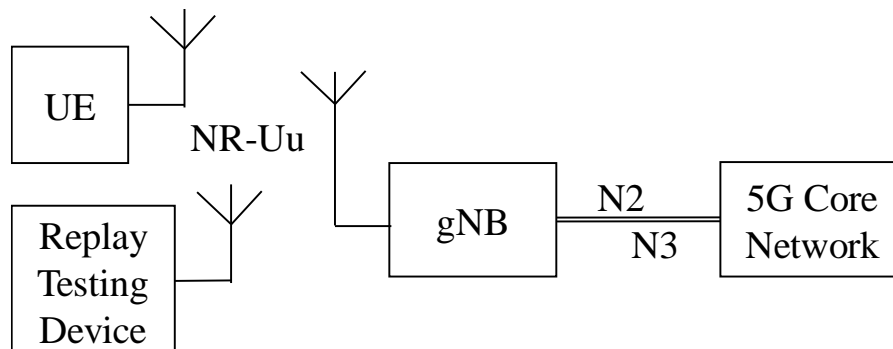
(d) 測試佈局：

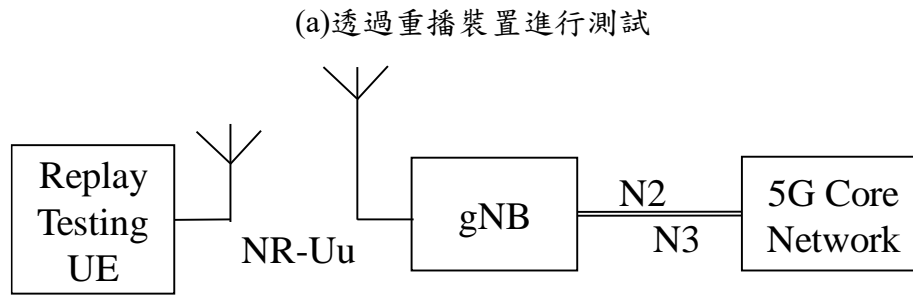
見(a)透過重播裝置進行測試



(b)透過具備重播功能的用戶設備進行測試

圖 16。



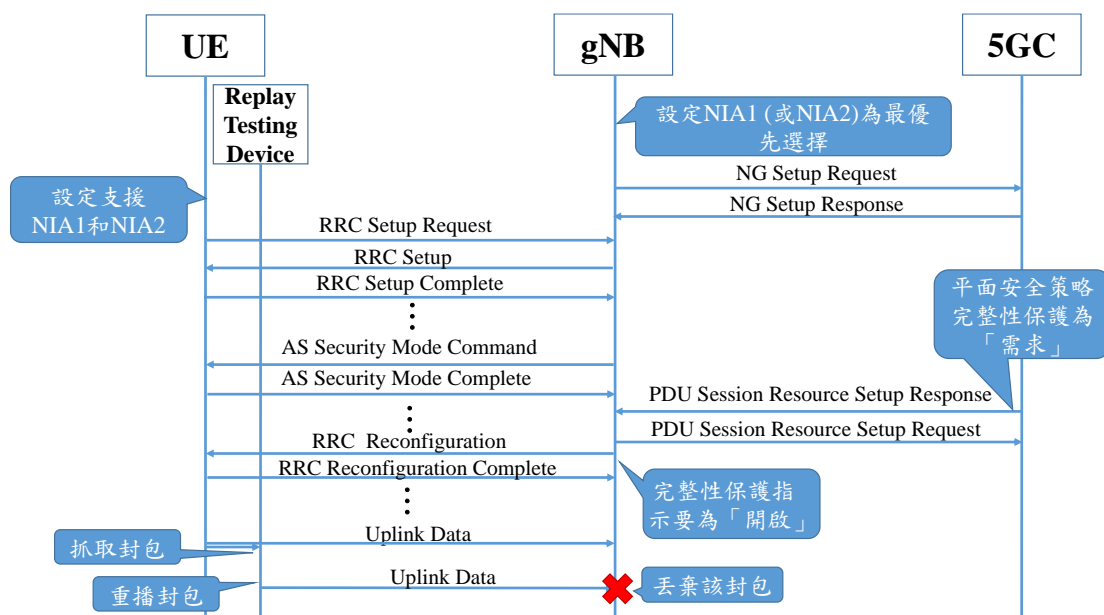


(b) 透過具備重播功能的用戶設備進行測試

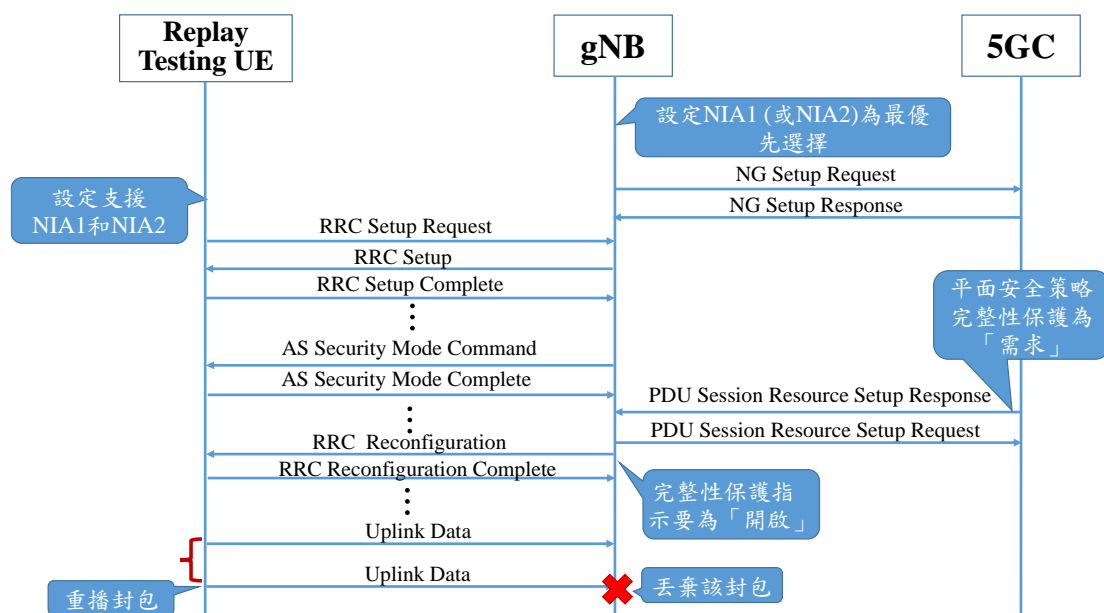
圖 16 用戶數據資料重播攻擊保護測試示意圖

(e) 測試步驟：

- (1) 在用戶設備設定支援 NIA1、NIA2 完整性安全演算法。
- (2) 在 gNB 端設定 NIA1 完整性安全演算法為最優先選擇。
- (3) 開始擷取 NG-RAN 介面封包。
- (4) 確認 gNB 與 5GC 間建立 NGAP 連線，且用戶設備註冊和傳送數據封包。
- (5) 從擷取的 NG-RAN 介面資料封包透過重播裝置選定特定用戶平面封包進行重播。而被重播的用戶平面封包它在 PDCP 層以上的訊息要和原始封包一樣。
- (6) 停止擷取 NG-RAN 介面封包。
- (7) 透過 NG-RAN 介面封包，確認 gNB 檢查重播的用戶平面封包在 PDCP 層帶有的 PDCP 計數是否重覆。
- (8) 將 gNB 端設定 NIA2 完整性安全演算法為最優先選擇重複(2)~(7)測試。



(a) 透過重播裝置進行測試



(b) 透過具備重播功能的用戶設備進行測試

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(7)，gNB 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 [6] 之第 5.3.3 小節與 3GPP TR 33.926 [7] 之第 D.2.2.2 小節，並參考 3GPP TS 33.511 [1] 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 gNB 間可以進行機密和完整性安全演算法設定。
- (2) 用戶設備、gNB 及 5GC 間可以成功建立 5G 連線。
- (3) SMF 要開啓用戶平面安全策略之用戶平面加密保護指示。
- (4) 測試人員可擷取 NG-RAN 介面封包，並分析 RRC 與用戶平面封包之 PDCP 層的內容。
- (5) 測試人員可擷取 N2 介面封包並分析該封包內容。

(d) 測試佈局：

見圖 18。

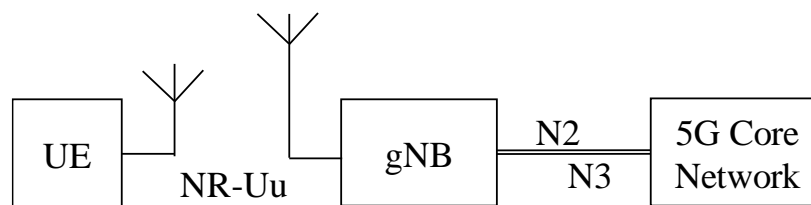


圖 18 用戶平面資料進行加密測試示意圖

(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 gNB 端設定 NEA1、NIA1 機密和完整性安全演算法為最優先選擇。
- (3) 開始擷取 NG-RAN 介面封包和 N2 介面封包。

- (4) 確認 gNB 與 5GC 間建立 NGAP 連線，且用戶設備註冊和傳送數據封包。
- (5) 停止擷取 NG-RAN 介面封包和 N2 介面封包。
- (6) 透過 NG-RAN 介面封包，確認用戶設備和 gNB 完成 RRC 信令安全驗證程序後。
- (7) 透過 N2 介面封包，確認 5GC 傳送給 gNB PDU Session Resource Set Up Request 帶有加密保護需求的安全資訊。
- (8) 透過 NG-RAN 介面封包，確認 gNB 傳送給用戶設備 RRC Reconfiguration 關閉加密保護指示是否符合程序(7) 加密保護需求。
- (9) 將 gNB 端設定 NEA2、NIA2 機密和完整性安全演算法為最優先選擇重複(2)~(8)測試。

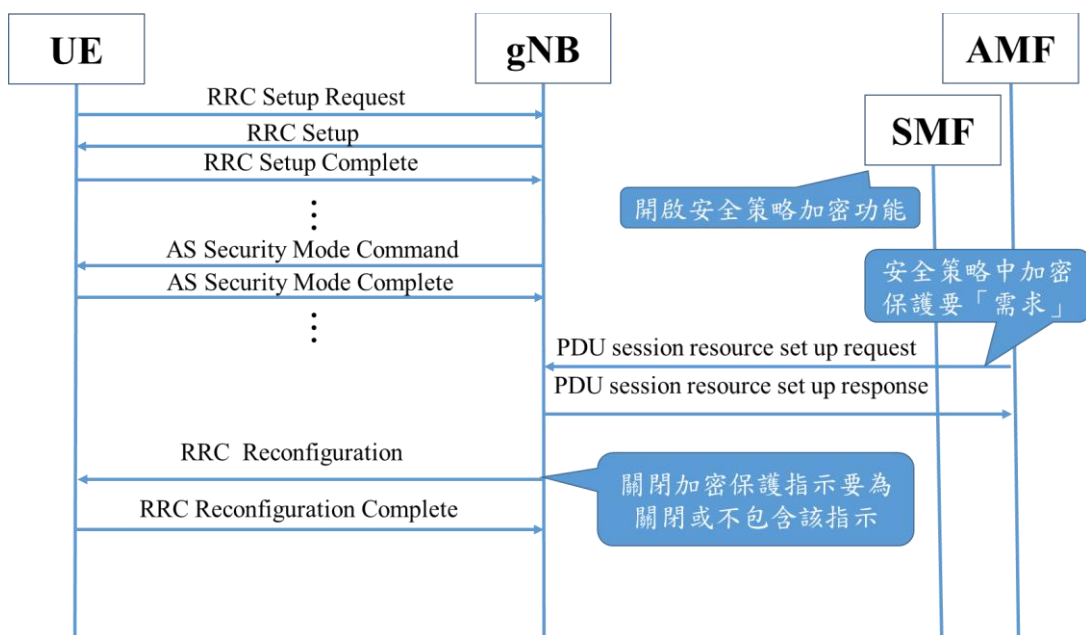


圖 19 用戶平面資料進行加密測試流程圖

(f) 測試結果：

- (1) 根據步驟(7)，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(8)，RRC Reconfiguration 關閉加密保護指示要符合程序(7) 加密保護需求為「關閉」或不包含該指示。

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 [6] 之第 5.3.2 小節與 3GPP TR 33.926 [7] 之第 D.2.2.8 小節，並參考 3GPP TS 33.511 [1] 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 gNB 間可以進行完整性安全演算法設定。
- (2) 用戶設備、gNB 及 5GC 間可以成功建立 5G 連線。
- (3) SMF 要開啓用戶平面安全策略之用戶平面完整性保護指示。
- (4) 測試人員可擷取 NG-RAN 介面封包，並分析 RRC 與用戶平面封包之 PDCP 層的內容。
- (5) 測試人員可擷取 N2 介面並分析該封包內容。

(d) 測試佈局：

見圖 20。

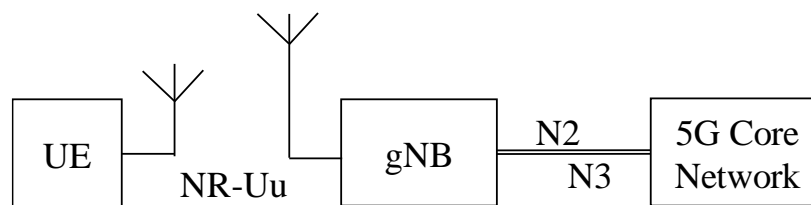


圖 20 用戶平面資料進行完整性保護測試示意圖

(e) 測試步驟：

- (1) 在用戶設備設定支援 NIA1 和 NIA2 完整性安全演算法。
- (2) 在 gNB 端設定 NIA1 完整性安全演算法為最優先選擇。
- (3) 開始擷取 NG-RAN 介面封包和 N2 介面封包。

- (4) 確認 gNB 與 5GC 建立 NGAP 連線，且用戶設備註冊和傳送數據封包。
- (5) 停止擷取 NG-RAN 介面封包和 N2 介面封包。
- (6) 透過 NG-RAN 介面封包，確認用戶設備和 gNB 完成 RRC 信令安全驗證程序後。
- (7) 透過 N2 介面封包，確認 5GC 傳送給 gNB PDU Session Resource Set Up Request 帶有完整性保護需求的安全資訊。
- (8) 透過 NG-RAN 介面封包，確認 gNB 傳送給用戶設備 RRC Reconfiguration 完整性保護指示是否符合程序(7) 加密保護需求。
- (9) 將 gNB 端設定 NIA2 完整性安全演算法為最優先選擇重複(2)~(8)測試。

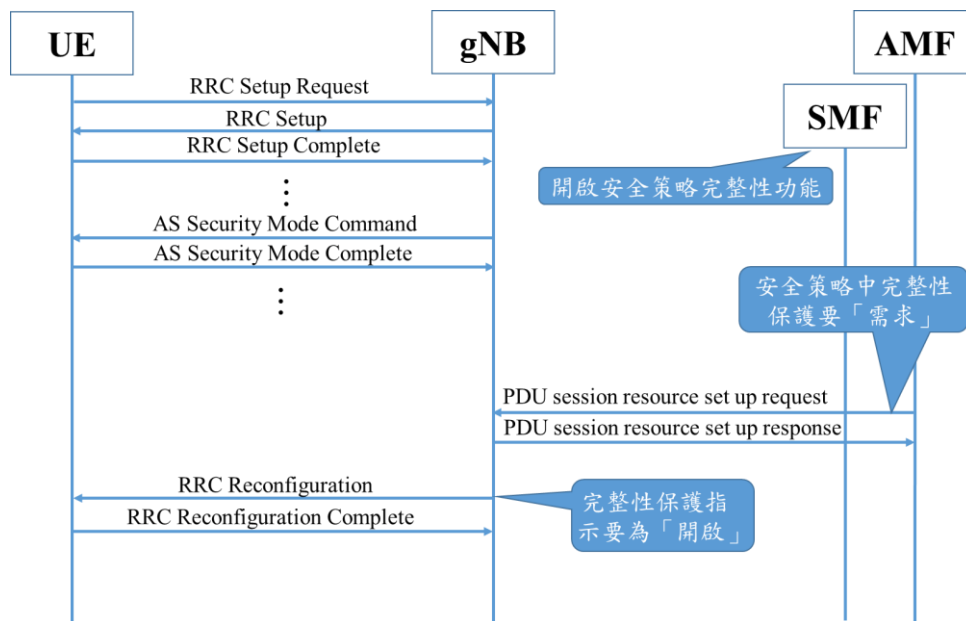


圖 21 用戶平面資料進行完整性保護測試流程圖

(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「需求」。
- (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 存取層安全演算法檢測

6.1.3.1 gNB 存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 [6] 之第 5.11.2 小節與 3GPP TR 33.926 [7] 之第 D.2.2.5 小節，並參考 3GPP TS 33.511 [1] 之第 4.2.2.1.12 小節。

(b) 測試目的：

驗證 gNB 存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 gNB 間可以進行機密和完整性安全演算法設定。
- (2) 用戶設備、gNB 及 5GC 間可以成功建立 5G 連線。
- (3) 測試人員可擷取 NR-RAN 介面封包，並分析 RRC 封包之 PDCP 層的內容。
- (4) 測試人員可擷取 N2 介面封包並分析該封包內容。

(d) 測試佈局：

見圖 22。

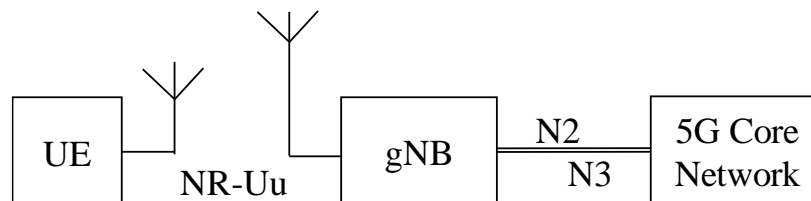


圖 22 加密和完整性演算法優先順序測試示意圖

(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 gNB 端設定 NEA1、NIA1 機密和完整性安全演算法為最優先選擇。
- (3) 開始擷取 NG-RAN 介面封包和 N2 介面封包。

- (4) 確認 gNB 與 5GC 建立 NGAP 連線，且用戶設備註冊上 5GC。
- (5) 停止擷取 NG-RAN 介面封包和 N2 介面封包。
- (6) 透過 N2 介面封包，確認 5GC 傳送給 gNB 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。
- (7) 透過 NG-RAN 介面封包，檢查 gNB 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。
- (8) 將 gNB 端設定 NEA2、NIA2 機密和完整性安全演算法為最優先選擇重複 (2)~(7)測試。

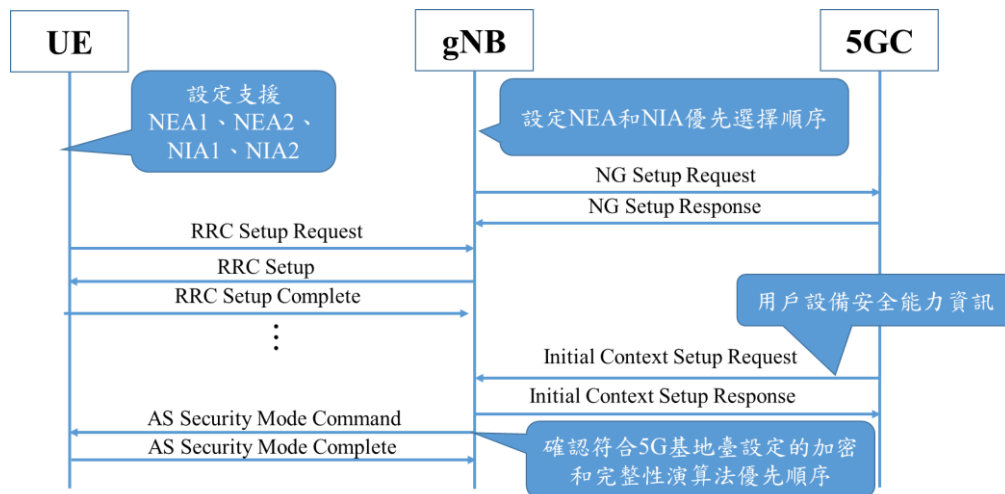


圖 23 加密和完整性演算法優先順序測試流程圖

(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 gNB 的安全演算法優先順序設定。

6.1.3.2 gNB 金鑰更新-封包資料匯聚通訊協定(PDCP)計數環繞

3GPP TS 33.501 [6] 已經刪除第 6.9.4.1 小節之資安測試需求。

6.1.3.3 gNB 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 [6] 之第 6.9.4.1 小節與 TS 38.331 [8] 之第 5.3.1.2 小節以及 3GPP TR 33.926 [7] 之第 D.2.2.7 小節，並參考 3GPP TS 33.511 [1] 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，gNB 金鑰 (K_{gNB}) 更新功能運作正常。

(c) 測試前提：

- (1) 用戶設備及 gNB 間可以進行完整性安全演算法設定。
- (2) 用戶設備、gNB 及 5GC 間可以成功建立 5G 連線。
- (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) 測試人員可擷取 NG-RAN 介面封包，並分析 RRC 與用戶平面封包之 PDCP 層的內容。
- (5) 測試人員可擷取 N2 介面封包並分析該封包內容。

(d) 測試佈局：

見圖 24。

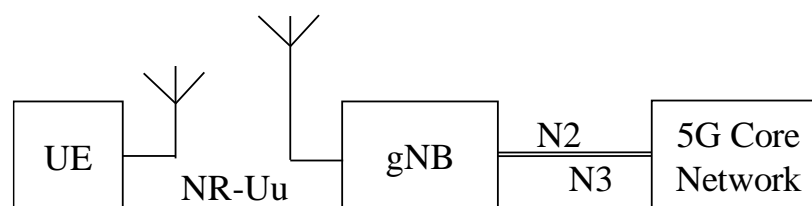


圖 24 gNB 金鑰更新測試示意圖

(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 gNB 端設定 NIA1 完整性安全演算法為最優先選擇。
- (3) 開始擷取 NG-RAN 介面封包。

- (4) 確認與 5GC 間建立 NGAP 連線，且用戶設備註冊上 5GC 和傳送數據資料。
- (5) 透過 NG-RAN 介面封包，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。
- (6) 停止擷取 NG-RAN 介面封包。
- (7) 透過 NG-RAN 介面封包，確認 gNB 發生 PDCP 重建進行 K_{gNB} 更新。

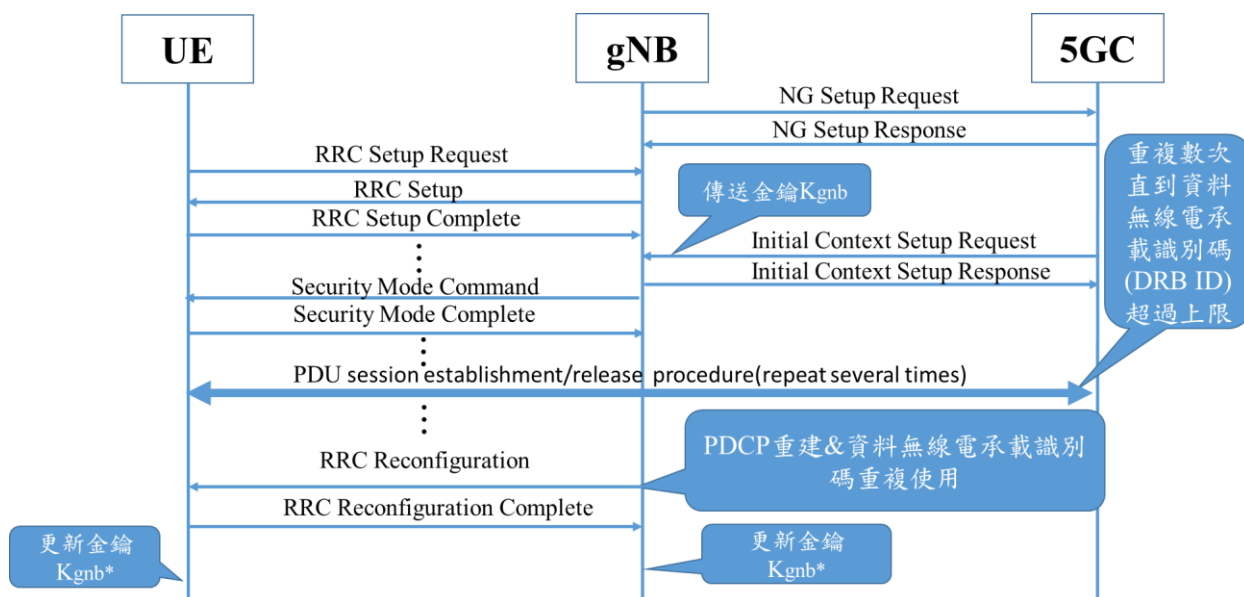


圖 25 gNB 金鑰更新測試流程圖

(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，在無線接取介面看到 PDCP 重建因此 gNB 進行 K_{gNB} 更新避免訊息洩露。

6.1.3.4 gNB 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 [6] 之第 6.10.2.1、6.10.2.2.1 小節與 3GPP TR 33.926 [7] 之第 D.2.2.7 小節，並參考 3GPP TS 33.511 [1] 之第 4.2.2.1.18 小節。

(b) 測試目的：

驗證次節點之 gNB 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 gNB 間可以進行完整性安全演算法設定。
- (3) 用戶設備、gNB 及 5GC 間可以成功建立 5G 連線。
- (4) 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」。
- (5) 測試人員可擷取 NG-RAN 介面封包，並分析 RRC 與用戶平面封包之 PDCP 層的內容。
- (6) 測試人員可擷取 Xn 封包並分析該封包內容
- (7) 測試人員可從用戶設備或 gNB 擷取安全金鑰 K_{SN}

(d) 測試佈局：

見圖 26。

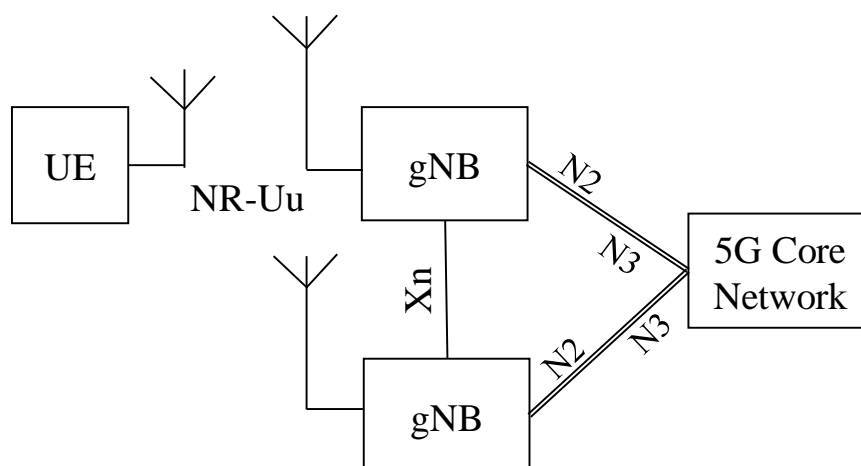


圖 26 gNB 金鑰更新測試示意圖

(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 gNB 端設定 NIA1 完整性安全演算法為最優先選擇。
- (3) 開始擷取 NG-RAN 介面和 Xn 介面封包。
- (4) 確認 gNB 與 5GC 建立 NGAP 連線，且用戶設備註冊上 5GC 和傳送數據資料。
- (5) 用戶設備建次節點之 gNB 連線。
- (6) 用戶設備在次節點對相同的無線電承載傳送 RRC 信令或用戶平面封包直至產生 PDCP 計數環繞 (wrap around)。
- (7) 停止擷取 NG-RAN 介面和 Xn 介面封包。
- (8) 透過 NG-RAN 介面和 Xn 介面，觀察 XnAP 是否啟動次節點金鑰更新流程及 K_{SN} 值狀態。

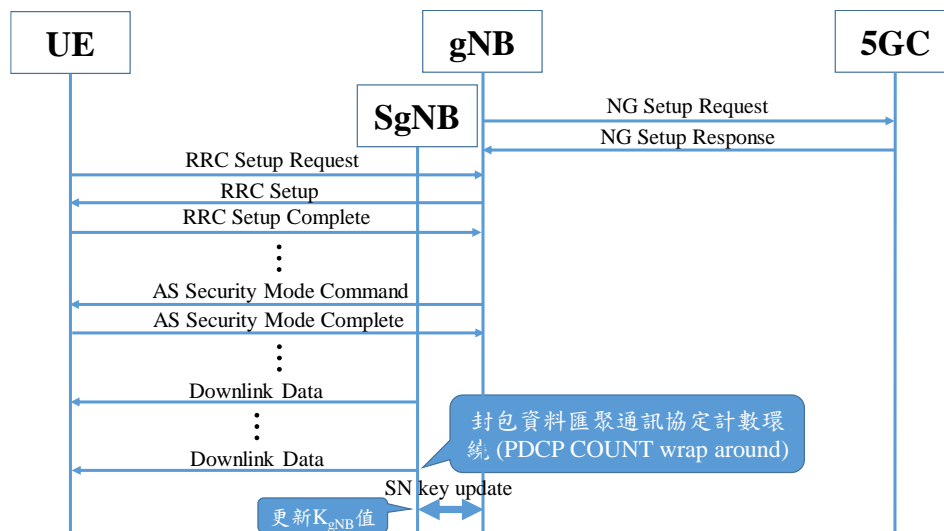


圖 27 gNB 金鑰更新測試流程圖

(f) 測試結果：

- (1) 根據步驟(8)，當發生 PDCP 計數環繞後，次節點之 gNB 會啟動更新金鑰 K_{SN} 避免訊息被洩漏

6.1.3.5 gNB 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 [6] 之第 6.10.2.1、6.10.2.2.1 小節與 3GPP TR 33.926 [7] 之第 D.2.2.7 小節，並參考 3GPP TS 33.511 [1] 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的通訊系統。
- (2) 用戶設備及 gNB 可進行完整性安全演算法設定。
- (3) 用戶設備、gNB 及 5GC 端可成功建立 5G 連線。
- (4) 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」。
- (5) 測試人員可擷取 NG-RAN 介面封包，並分析 RRC 與用戶平面封包之 PDCP 層的內容。
- (6) 測試人員可擷取 Xn 封包並分析該封包內容
- (7) 測試人員可從用戶設備或 gNB 擷取安全金鑰 K_{SN}

(d) 測試佈局：

見圖 28。

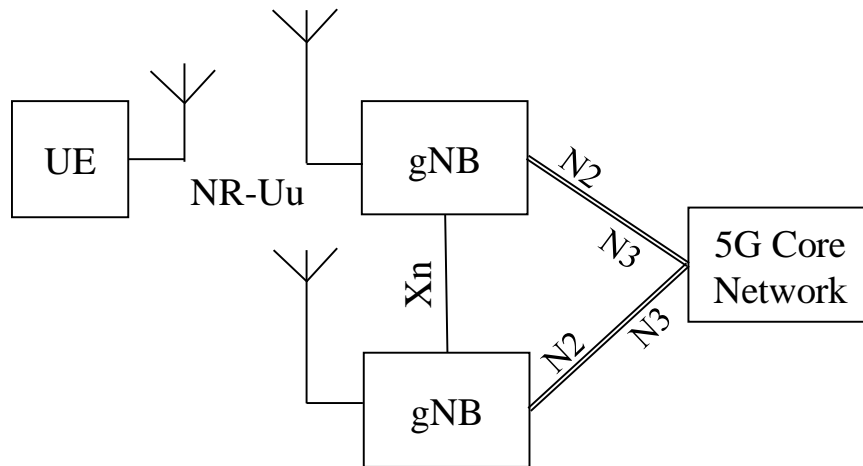


圖 28 gNB 金鑰更新測試示意圖

(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 gNB 端設定 NIA1 完整性安全演算法為最優先選擇。
- (3) 開始擷取 NG-RAN 介面和 Xn 介面封包。
- (4) 確認 gNB 與 5GC 間建立 NGAP 連線，且用戶設備註冊上 5GC 和傳送數據資料。
- (5) 用戶設備建次節點之 gNB 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) 停止擷取 NG-RAN 介面和 XnAP 封包。
- (8) 觀察 Xn 應用協定是否啟動次節點金鑰更新流程及 KSN 值狀態。

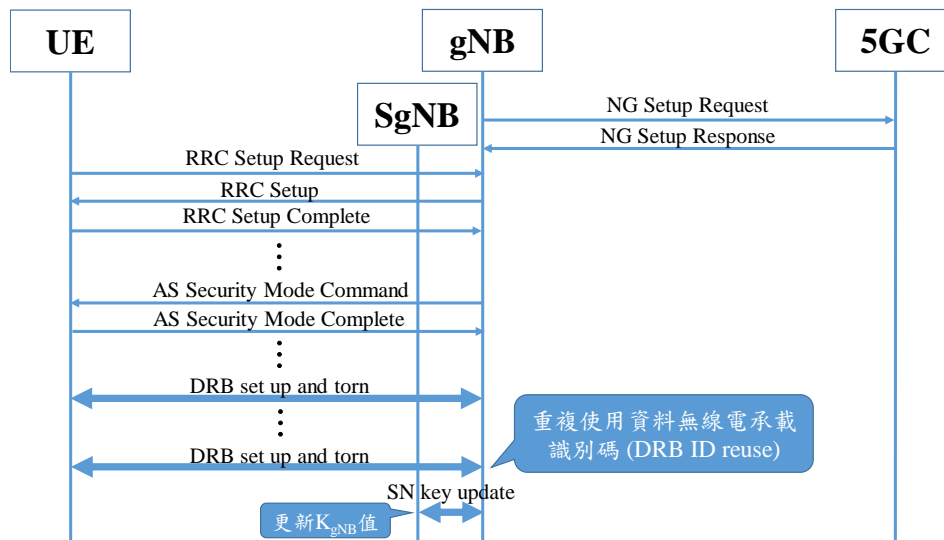


圖 29 gNB 金鑰更新測試流程圖

(f) 測試結果：

- (1) 根據步驟(8)，當發生重複使用資料無線電承載識別碼後，SN gNB 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 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 [6] 之第 6.7.3.1 小節與 3GPP TR 33.926 [7] 之第 D.2.2.6 小節，並參考 3GPP TS 33.511 [1] 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 gNB 及目的 gNB 可以進行存取層安全演算法設定。
- (2) gNB 可以支援 Xn 介面換手

- (3) 用戶設備、gNB 及 5GC 間可以成功建立 5G 連線。
- (4) 測試人員可擷取 N2 介面封包並分析其內容。
- (5) 測試人員可擷取 Xn 介面封包並分析其內容。

(d) 測試佈局：

見圖 30。

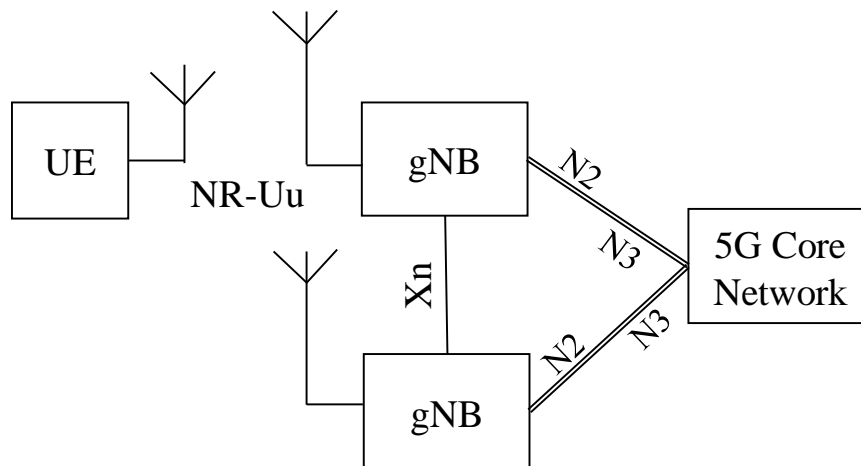


圖 30 防範 Xn 交遞中的降階攻擊測試示意圖

(e) 測試步驟：

- (1) 在用戶設備設定支援 NEA1、NEA2、NIA1、NIA2 機密和完整性安全演算法。
- (2) 在來源和目的 gNB 端設定 NEA1、NIA1 機密和完整性安全演算法為最優先選擇。
- (3) 開始擷取 N2 介面和 Xn 介面的封包。
- (4) 確認來源 gNB 及目的 gNB 分別與 5GC 建立 NGAP 連線，來源 gNB 及目的 gNB 間建立 XnAP 連線，且用戶設備透過來源 gNB 註冊上 5GC。
- (5) 用戶設備進行換手，確認用戶設備、來源和目的 gNB 和 5GC 完成 Xn 介面換手程序。
- (6) 停止擷取 N2 介面和 Xn 介面的封包。

(7) 透過 N2 介面的封包，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。

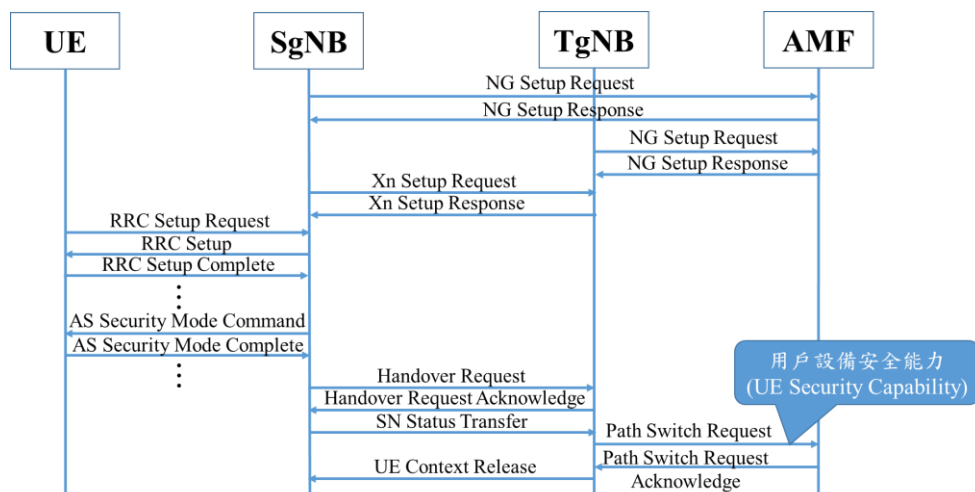


圖 31 防範 Xn 交遞中的降階攻擊測試流程圖

(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 介面交遞中存取層安全演算法選擇

(a) 測試依據：

依據 3GPP TS 33.501 [6] 之第 6.7.3.1、6.7.3.2 小節與 3GPP TR 33.926 [7] 之第 D.2.2.5 小節，並參考 3GPP TS 33.511 [1] 之第 4.2.2.1.15 小節。

(b) 測試目的：

驗證當發生 Xn 交遞時存取層安全演算法選擇機制。

(c) 測試前提：

(1) 用戶設備、來源 gNB 及目的 gNB 間可以進行存取層安全演算法設定。

(2) gNB 可以支援 Xn 介面換手。

- (3) 用戶設備、gNB 及 5GC 可以成功建立 5G 連線。
- (4) 測試人員可擷取 NG-RAN 介面封包，並分析 RRC 之 PDCP 層的內容。
- (5) 測試人員可擷取 N2 介面封包並分析其內容。
- (6) 測試人員可擷取 Xn 介面封包並分析其內容。

(d) 測試佈局：

見圖 32。

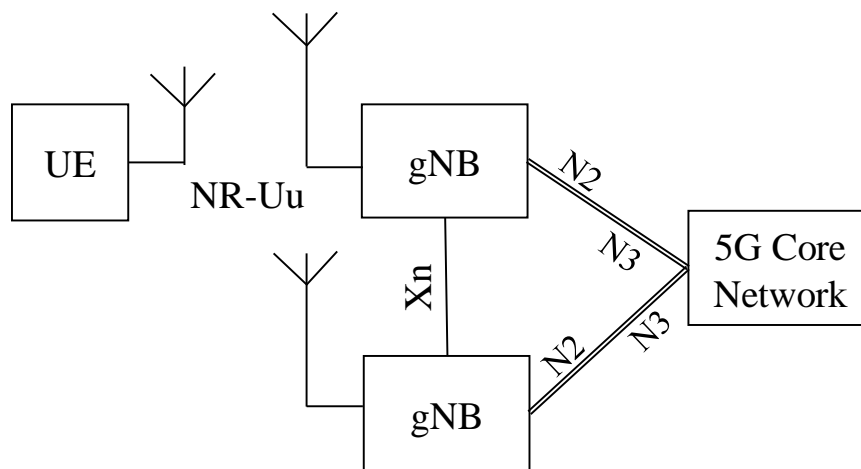


圖 32 在 Xn 交遞中存取層安全演算法選擇測試示意圖

(e) 測試步驟：

- (1) 在用戶設備設定支援 NEA1、NEA2、NIA1、NIA2 機密和完整性安全演算法。
- (2) 在來源和目的 gNB 端設定 NEA1、NIA1 機密和完整性安全演算法為最優先選擇。
- (3) 開始擷取 NG-RAN 介面、N2 介面和 Xn 介面的封包。
- (4) 確認來源 gNB 及目的 gNB 與 5GC 建立 NG-RAN 連線，且用戶設備透過來源 gNB 註冊上 5GC。
- (5) 用戶設備進行換手，確認用戶設備、來源和目的 gNB 和 5GC 完成 Xn 介面換手程序。

(6) 停止擷取 NG-RAN 介面、N2 介面和 Xn 介面的封包。

(7) 透過 NG-RAN 介面或 Xn 介面，檢查 RRC Reconfiguration 或 Handover Request Acknowledge(Handover Command)中的目的 gNB 的加密和完整性安全演算法。

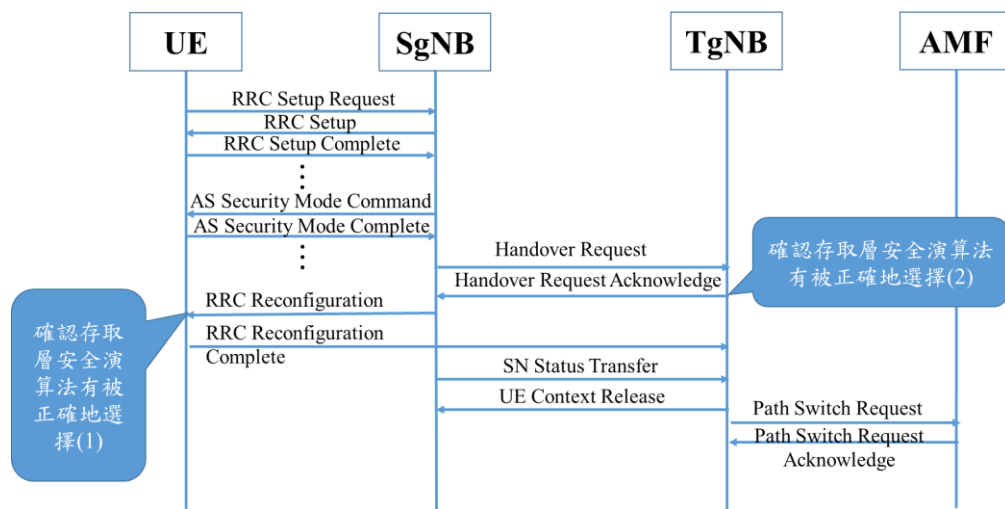


圖 33 在 Xn 交遞中存取層安全演算法選擇測試流程圖

(f) 測試結果：

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

6.1.5 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

(a) 測試依據：

依據 3GPP TS 33.501 [6] 之第 9.2 小節與 3GPP TR 33.926 [7] 之第 D.2.2.1 小節，並參考 3GPP TS 33.511 [1] 之第 4.2.2.1.16 小節與 3GPP TS 33.210 [4] 之第 5.3.3 和 5.3.4 小節。

(b) 測試目的：

驗證 N2 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 gNB 間可以進行存取層安全演算法設定。
- (2) 安全閘道器 (Security Gateway) 用戶端及伺服器端都可以支援 IKEv2，並可進行 IPsec 安全演算法設定。
- (3) 安全閘道器用戶端及伺服器之間可以成功建立 IPsec 連線。
- (4) 用戶設備、gNB 及 5GC 間可以透過 IPsec 成功建立 5G 連線。
- (5) 測試人員可擷取並解密 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。

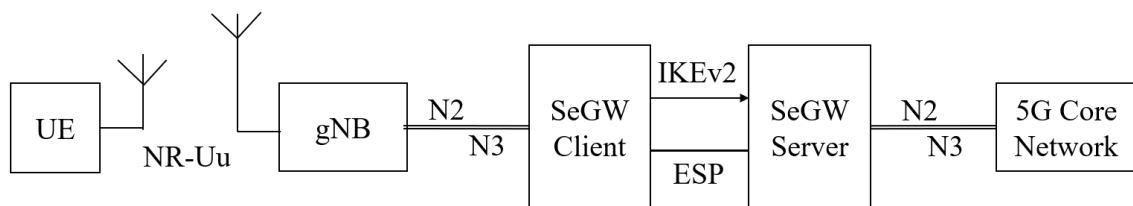


圖 34 控制平面資料在 N2 介面機密性保護測試示意圖

(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 gNB 端設定 NEA1、NIA1 機密和完整性安全演算法為最優先選擇。
- (3) 開始擷取 IPsec 介面封包。

- (4) 安全閘道器的用戶端和伺服器建立 IPsec 連線。
- (5) gNB 與 5GC 透過 IPsec 建立下一代應用協定連線，並進行用戶設備註冊。
- (6) 停止擷取 IPsec 介面封包。
- (7) 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。
- (8) 透過網際網路安全協定介面封包，確認使用封裝安全承載量進行資料傳輸並解密其封包。

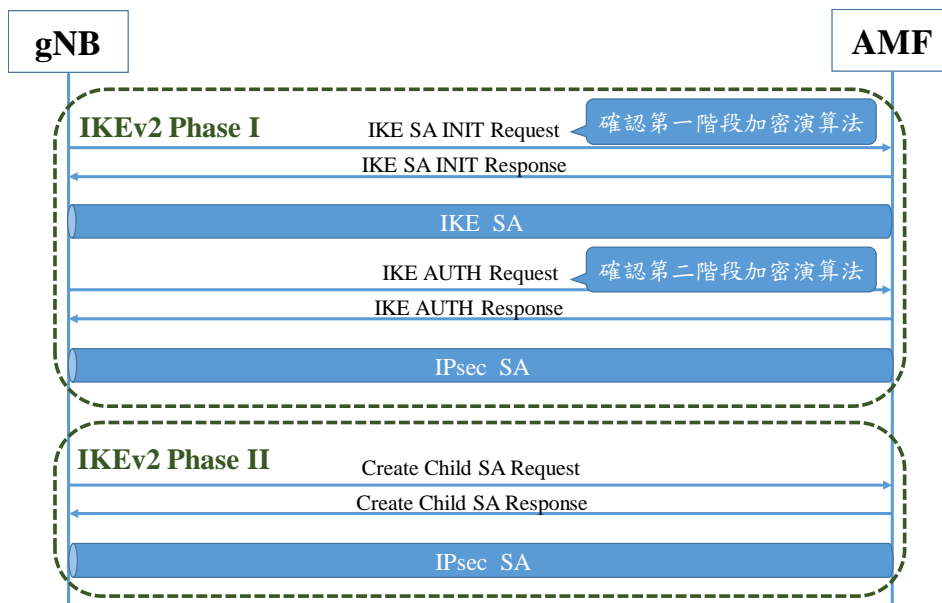


圖 35 控制平面資料在 N2 介面機密性保護測試流程圖

(f) 測試結果：

- (1) 根據步驟(7)，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(7)，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(8)，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，將其解密後得到下一代應用協定資料封包。

6.1.5.2 用戶平面資料在 N3 介面的機密性保護

(a) 測試依據：

依據 3GPP TS 33.501 [6] 之第 9.3 小節與 3GPP TR 33.926 [7] 之第 D.2.2.2 小節，並參考 3GPP TS 33.513 [2] 之第 4.2.2.1 小節與 3GPP TS 33.210 [4] 之第 5.3.3 和 5.3.4 小節。

(b) 測試目的：

驗證 N3 介面控制平面資料符合 IPsec (IPsec) 加密和認證達到完整性保護。

(c) 測試前提：

- (1) 用戶設備及 gNB 間可以進行存取層安全演算法設定。
- (2) 安全閘道器 (Security Gateway) 的用戶端及伺服器之間可以成功建立 IPsec 連線。

- (3) 安全閘道器的用戶端及伺服器都可以支援 IKEv2，並可進行 IPsec 安全演算法設定。
- (4) 用戶設備、gNB 及 5GC 間可以透過 IPsec 成功建立 5G 連線。
- (5) 測試人員可擷取並解密 IPsec 介面封包，並分析 ISAKMP 與封裝安全承載量內容。

(d) 測試佈局：

見圖 36。

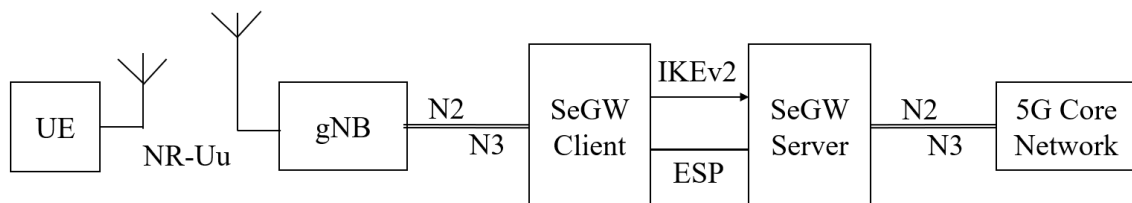


圖 36 控制平面資料在 N3 介面機密性保護測試示意圖

(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 gNB 端設定 NEA1、NIA1 機密和完整性安全演算法為最優先選擇。
- (3) 開始擷取 IPsec 介面封包。
- (4) 安全閘道器的用戶端和伺服器建立 IPsec 連線。
- (5) gNB 與 5GC 透過 IPsec 建立 NGAP 連線，並進行用戶設備註冊和傳送數據資料。
- (6) 停止擷取實際網路安全協定介面封包。
- (7) 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。

(8) 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出其封包。

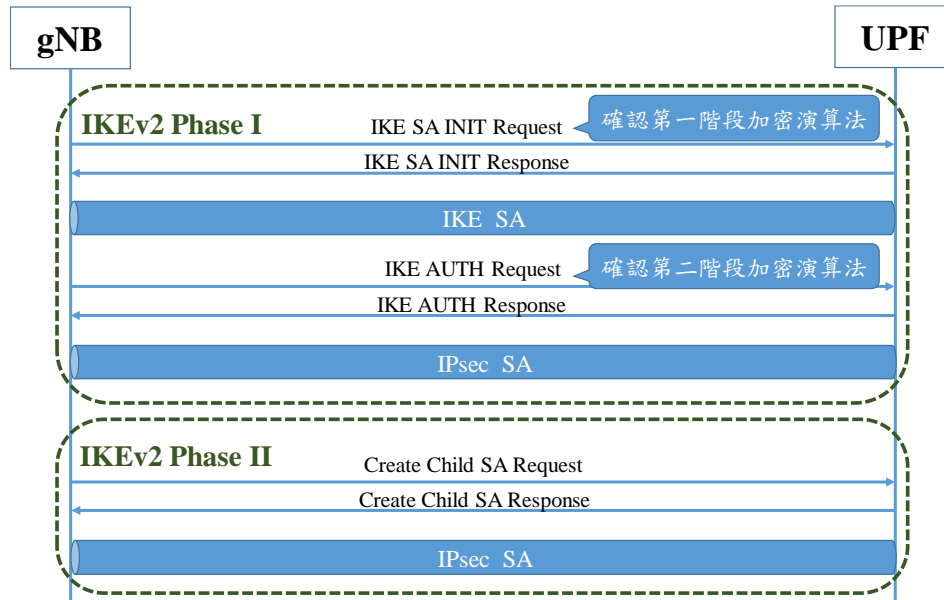


圖 37 控制平面資料在 N3 介面機密性保護測試流程圖

(f) 測試結果：

(1) 根據步驟(7)，IKE-SA-INIT 請求信令中含有 IKEv2 的第一階段加密演算法需要符合以下標準。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(7)，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 的第二階段加密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，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(7)，封裝安全承載量資料封包是由 IKEv2 的第二階段加密演算法進行機密性保護，將其解密後得到 N3 應用協定資料封包。

6.1.5.3 控制平面資料在 Xn 介面的機密性保護

(a) 測試依據：

依據 3GPP TS 33.501 [6] 之第 9.4 小節與 3GPP TR 33.926 [7] 之第 D.2.2.1 小節，並參考 3GPP TS 33.511 [1] 之第 4.2.2.1.16 小節與 3GPP TS 33.210 [4] 之第 5.3.3 和 5.3.4 小節。

(b) 測試目的：

驗證 Xn 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、來源 gNB 及目的 gNB 間可以進行存取層安全演算法設定。
- (2) 安全閘道器 (Security Gateway) 的用戶端及伺服器之間可以成功建立 IPsec 連線。
- (3) Xn 介面相關的安全閘道器的用戶端及用戶端之間可以成功建立 IPsec 連線。
- (4) Xn 介面相關的安全閘道器的用戶端及伺服器都可以支援 IKEv2 並可進行 IPsec 安全演算法設定。

(5) Xn 介面相關的安全閘道器的用戶端及用戶端都可以支援 IKEv2 並可進行 IPsec 安全演算法設定。

(6) gNB 可支援 Xn 介面換手。

(7) 用戶設備、gNB 及 5GC 端可透過 IPsec 成功建立 5G 連線。

(8) 測試人員可擷取並解密 IPsec 介面封包，並分析 ISAKMP 與封裝安全承載量內容。

(d) 測試佈局：

見圖 38。

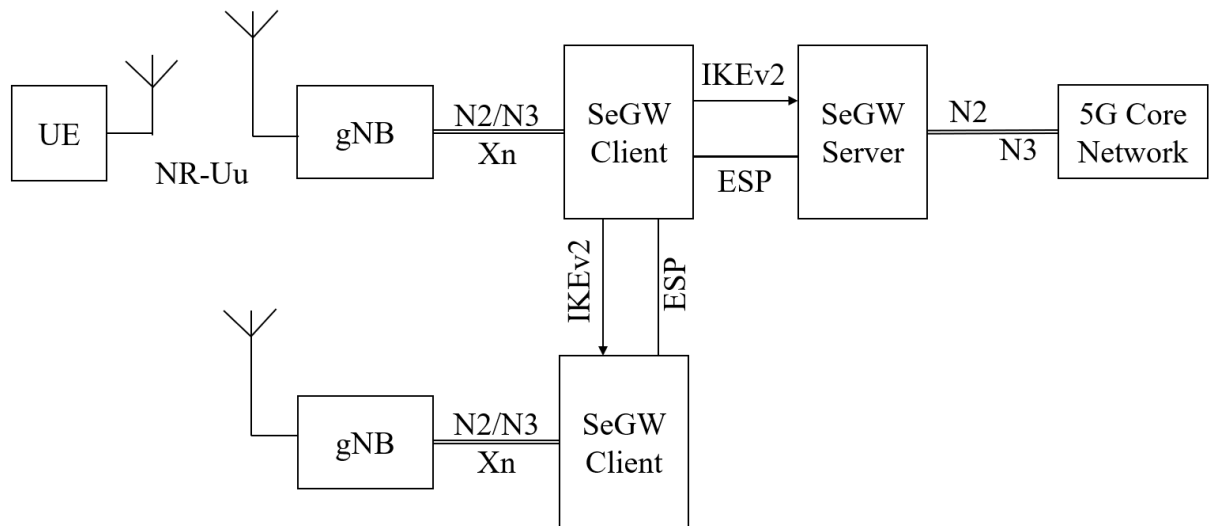


圖 38 控制平面資料在 Xn 介面機密性保護測試示意圖

(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) 在來源和目的 gNB 端設定 NEA1、NIA1 機密和完整性安全演算法為最優先選擇。

(3) 開始擷取 Xn 介面相關 IPsec 介面封包。

- (4) 安全閘道器的用戶端和伺服器建立 IPsec 連線。
- (5) gNB 與 5GC 透過 IPsec 建立 NGAP 連線，並進行用戶設備註冊和換手。
- (6) 停止擷取 IPsec 封包。
- (7) 透過 IPsec 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。
- (8) 透過 IPsec 封包，確認使用封裝安全承載量進行資料傳輸並解密出其封包。

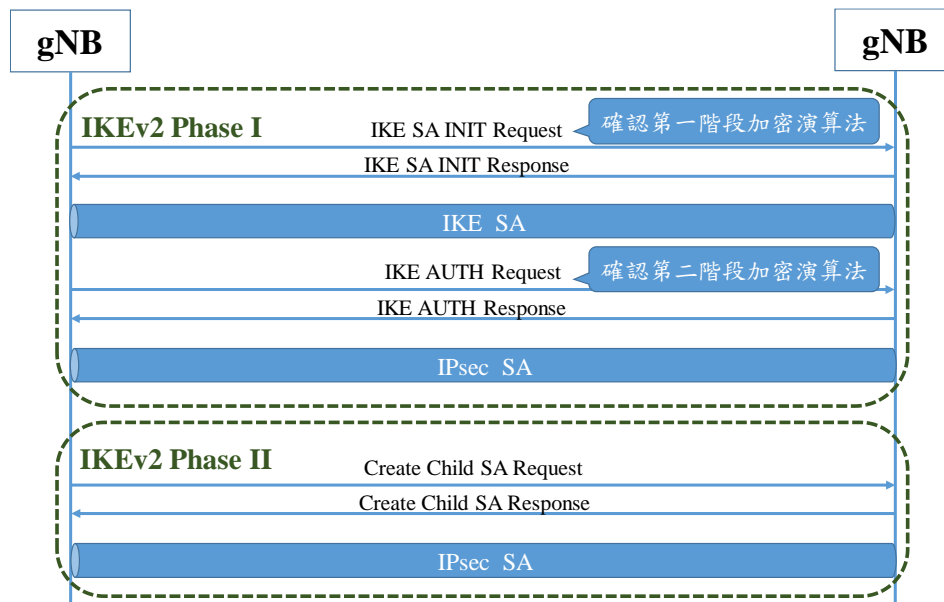


圖 39 控制平面資料在 Xn 介面機密性保護測試流程圖

(f) 測試結果：

- (1) 透過步驟(7)，IKE-SA-INIT 請求信令中含有 IKEv2 的第一階段加密演算法需要符合以下標準。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) 透過步驟(7)，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 的第二階段加密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，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) 透過步驟(8)，封裝安全承載量資料封包是由 IKEv2 的第二階段加密演算法進行機密性保護，將其解密後得到 Xn 應用協定資料封包。

6.1.5.4 控制平面資料在 N2 介面的完整性保護

(a) 測試依據：

依據 3GPP TS 33.501 [6] 之第 9.2 小節與 3GPP TR 33.926 [7] 之第 D.2.2.2 小節，並參考 3GPP TS 33.511 [1] 之第 4.2.2.1.17 小節與 3GPP TS 33.210 [4] 之第 5.3.3 和 5.3.4 小節。

(b) 測試目的：

驗證 N2 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 gNB 間可以進行存取層安全演算法設定。

- (2) 安全閘道器 (Security Gateway) 的用戶端及伺服器之間可以支援 IKEv2，並可進行際網路安全協定安全演算法設定。
- (3) 安全閘道器用戶端及伺服器端之間可以成功建立 IPsec 連線。
- (4) 用戶設備、gNB 及 5GC 間可以透過 IPsec 成功建立 5G 連線。
- (5) 測試人員可擷取並解密 IPsec 封包，並分析 ISAKMP 與封裝安全承載量內容。

(d) 測試佈局：

見圖 40。

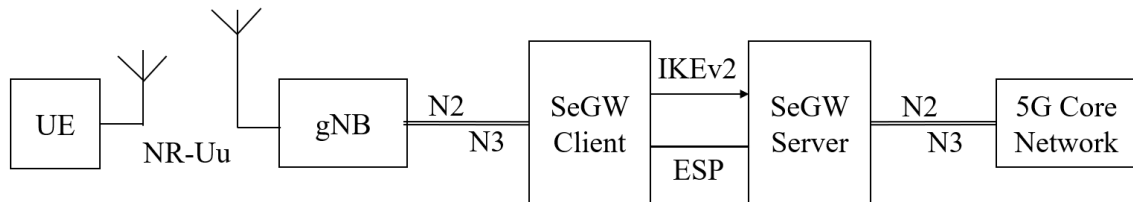


圖 40 控制平面資料在 N2 介面完整性保護測試示意圖

(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 gNB 端設定 NEA1、NIA1 機密和完整性安全演算法為最優先選擇。
- (3) 開始擷取 IPsec 封包。
- (4) 安全閘道器的伺服器和伺服器建立 IPsec 連線。
- (5) gNB 與 5GC 透過 IPsec 建立 NGAP 連線，並進行用戶設備註冊。
- (6) 停止擷取 IPsec 封包。
- (7) 透過 IPsec 封包，確認完成 IKE-SA-INIT 和 IKE-AUTH 程序並解密檢查其中之完整性演算法。

(8) 透過 IPsec 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。

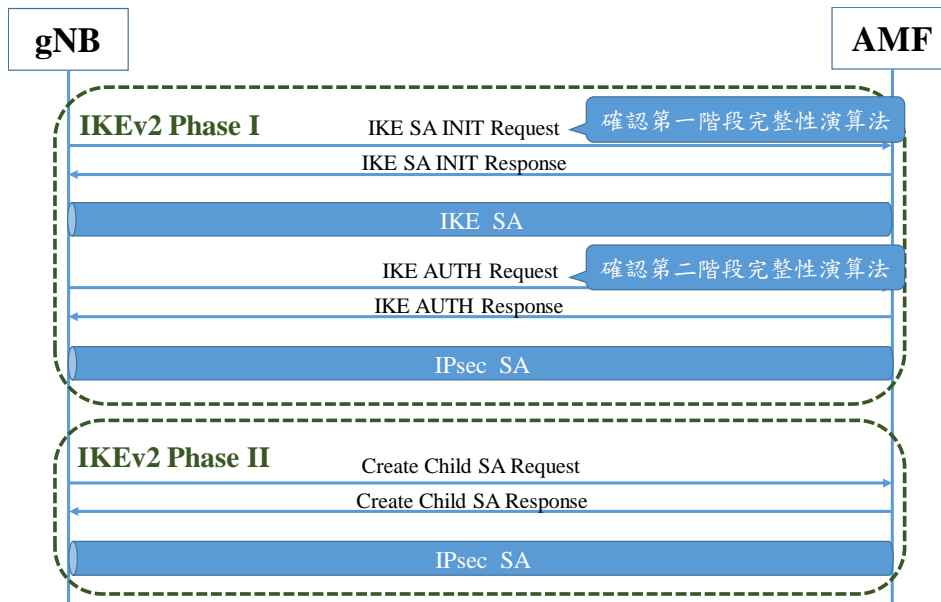


圖 41 控制平面資料在 N2 介面完整性保護測試流程圖

(f) 測試結果：

(1) 透過步驟(7)，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(7)，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(8)，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，將其解密後得到下一代應用協定資料封包。

6.1.5.5 用戶平面資料在 N3 介面的完整性保護

(a) 測試依據：

依據 3GPP TS 33.501 [6] 之第 9.3 小節與 3GPP TR 33.926 [7] 之第 D.2.2.2 小節，並參考 3GPP TS 33.513 [2] 之第 4.2.2.2 小節與 3GPP TS 33.210 [4] 之第 5.3.3 和 5.3.4 小節。

(b) 測試目的：

驗證 N3 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 gNB 間可以進行存取層安全演算法設定。
- (2) 安全閘道器 (Security Gateway) 的用戶端及伺服器之間可以成功建立 IPsec 連線。
- (3) 安全閘道器的用戶端及伺服器端都可以支援 IKEv2，並可進行 IPsec 安全演算法設定。
- (4) 用戶設備、gNB 及 5GC 間可以透過 IPsec 成功建立 5G 連線。
- (5) 測試人員可擷取並解密 IPsec 介面封包，並分析 ISAKMP 與封裝安全承載量內容。

(d) 測試佈局：

見圖 42。

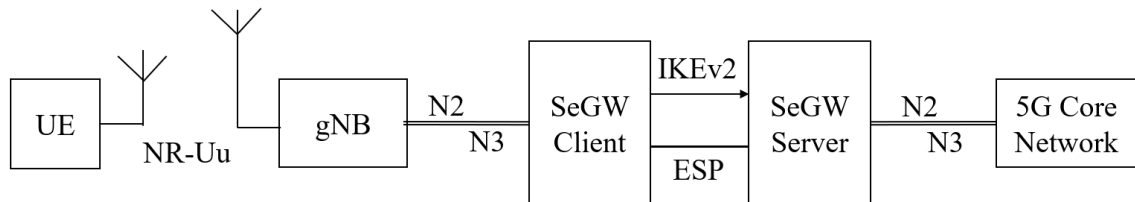


圖 42 控制平面資料在 N3 介面機密性保護測試示意圖

(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 gNB 端設定 NEA1、NIA1 機密和完整性安全演算法為最優先選擇。
- (3) 開始擷取 IPsec 封包。
- (4) 安全閘道器的用戶端和伺服器端建立實際網路安全協定連線。
- (5) gNB 與 5GC 透過 IPsec 建立 NGAP 連線，並進行用戶設備註冊和傳送數據資料。
- (6) 停止擷取實際網路安全協定介面封包。
- (7) 透過 IPsec 封包，確認完成 IKE-SA-INIT 和 IKE-AUTH 程序並解密檢查其中之完整性演算法。
- (8) 透過 IPsec 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。

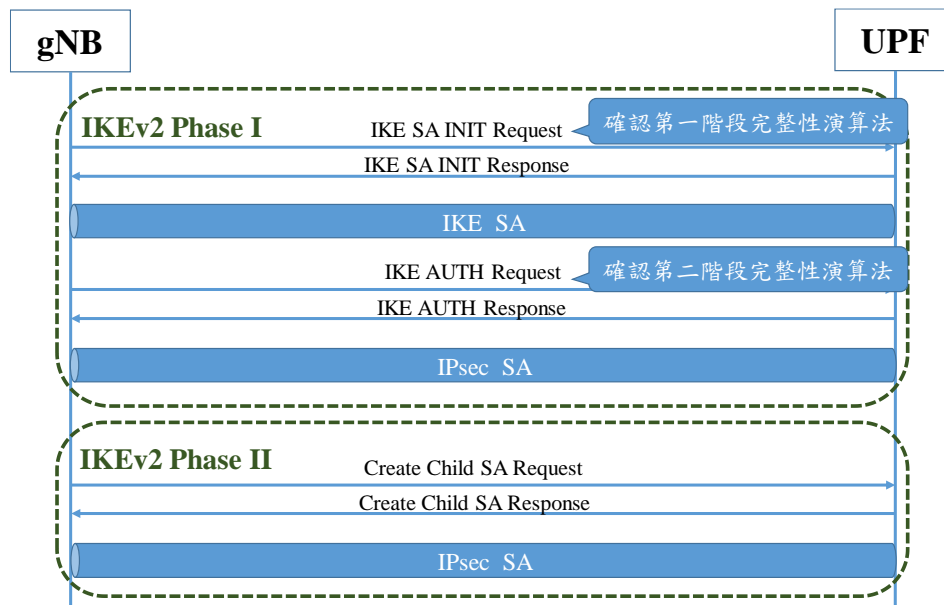


圖 43 控制平面資料在 N3 介面完整性保護測試流程圖

(f) 測試結果：

- (1) 根據步驟(7)，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) 根據步驟(7)，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，標記為+代表演算法強度更強。

- i AUTH_HMAC_SHA2_256_128 - 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 –Shall
- iv AUTH_HMAC_SHA2_512_256 - Should

(3) 根據步驟(8)，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 N3 應用協定資料封包。

6.1.5.6 控制平面資料在 Xn 介面的完整性保護

(a) 測試依據：

依據 3GPP TS 33.501 [6] 之第 9.4 小節與 3GPP TR 33.926 [7] 之第 D.2.2.2 小節，並參考 3GPP TS 33.511 [1] 之第 4.2.2.1.17 小節與 3GPP TS 33.210 [4] 之第 5.3.3 和 5.3.4 小節。

(b) 測試目的：

驗證 Xn 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、來源 gNB 及目的 gNB 間可以進行存取層安全演算法設定。
- (2) Xn 介面相關的安全閘道器 (Security Gateway) 的用戶端及伺服器之間可以成功建立 IPsec 連線。
- (3) Xn 介面相關的安全閘道器的用戶端及用戶端之間可以成功建立 IPsec 連線。
- (4) Xn 介面相關的安全閘道器的用戶端及伺服器都可以支援 IKEv2 並可進行 IPsec 安全演算法設定。
- (5) 下一代 Xn 介面相關的安全閘道器的用戶端及用戶端都可以支援 IKEv2 並可進行 IPsec 安全演算法設定。
- (6) gNB 可以支援 Xn 介面換手。

(7) 用戶設備、gNB 及 5GC 間可以透過 IPsec 成功建立 5G 連線。

(8) 測試人員可擷取並解密 IPsec 介面封包，並分析 ISAKMP 與封裝安全承載量內容。

(d) 測試佈局：

見圖 44。

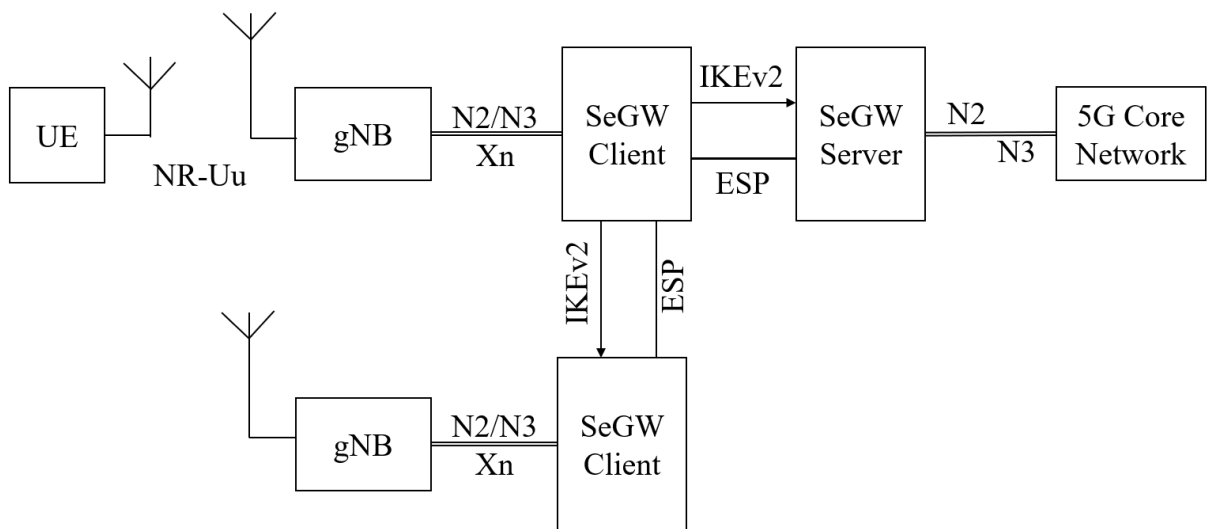


圖 44 控制平面資料在 Xn 介面完整性保護測試示意圖

(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) 在來源和目的 gNB 端設定 NEA1、NIA1 機密和完整性安全演算法為最優先選擇。

(3) 開始擷取 Xn 介面相關 IPsec 封包。

(4) 安全閘道器的用戶端和伺服器端建立 IPsec 連線。

(5) gNB 與 5GC 透過 IPsec 建立 XnAP 連線，並進行用戶設備註冊和換手。

(6) 停止擷取 IPsec 封包。

(7) 透過 IPsec 封包，確認完成 IKE-SA-INIT 和 IKE-AUTH 程序並解密檢查其中之完整性演算法。

(8) 透過 IPsec 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。

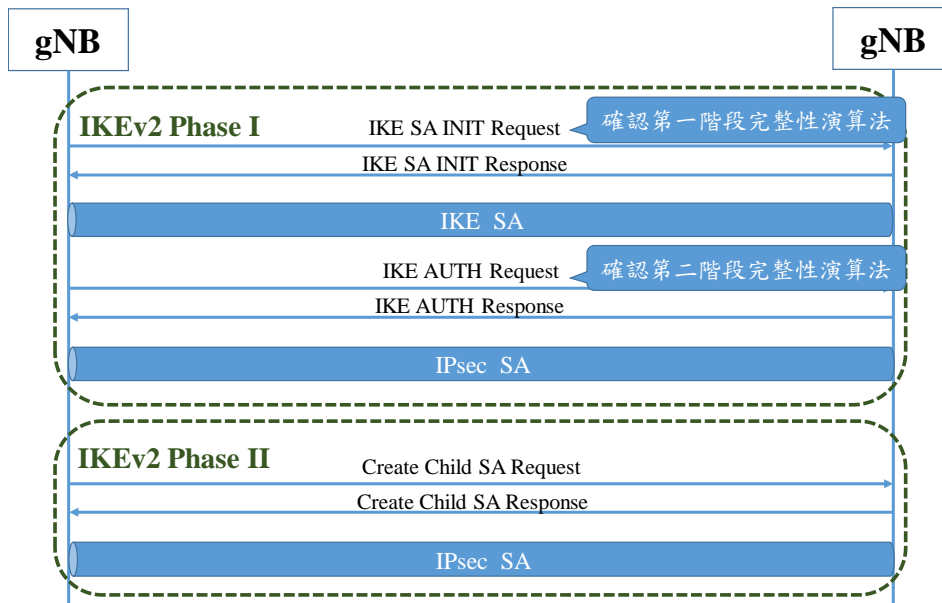


圖 45 控制平面資料在 Xn 介面完整性保護測試流程圖

(f) 測試結果：

(1) 透過步驟(7)，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(7)，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 a 16 octet ICV with 128-bit key length – Shall
- iii AES-GCM with a 16 octet ICV with 256-bit key length – Shall
- iv AUTH_HMAC_SHA2_512_256 - Should

(3) 透過步驟(8)，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 Xn 應用協定資料封包。

6.1.6 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

(a) 測試依據：

參考 3GPP TS 33.511 [1] 之第 4.2.6.2.4 小節與 3GPP TS 33.117 [2] 之第 4.2.6.2.4 小節。

(b) 測試目的：

確認 gNB 擁有過濾特定 GTP-U 封包的能力。

(c) 測試前提：

- (1) gNB 具備一個以上 GTP-U 資訊的網路傳輸介面。
- (2) gNB 可以設定 GTP-U 的過濾功能。
- (3) 可以抓取 gNB 之網路傳輸介面(如 N3 介面)的 GTP-U 封包。

(d) 測試佈局：

見圖 48。

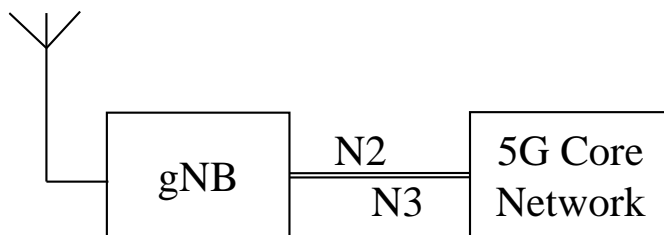


圖 46 GTP-U 封包過濾功能測試示意圖

(e) 測試步驟：

- (1) 設定 gNB 的一個 N3 介面只允許其能夠接收 GTP-U Echo Request 信令。
- (2) UPF 對 gNB 設定允許接收之 N3 介面傳送 GTP-U Echo Request 信令，UPF 成功收到來自 gNB 發送之 GTP-U Echo Response 信令。
- (3) 設定 gNB 的一個 N3 介面禁止其能夠接收任何 GTP-U 信令。
- (4) UPF 對 gNB 設定禁止接收之 N3 介面傳送 GTP-U Echo Request 信令，gNB 拋棄該 GTP-U Echo Request 信令，故 UPF 將不會收到 GTP-U Echo Response。

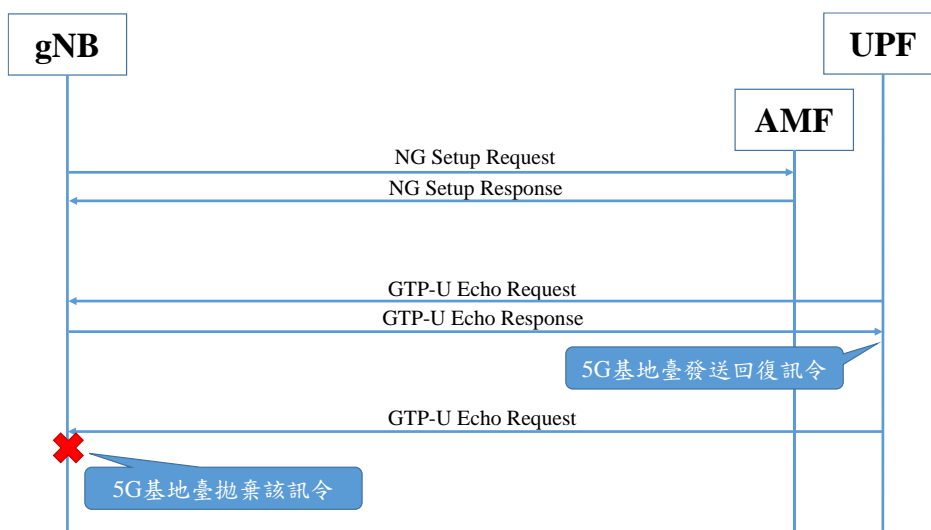


圖 47 GTP-U 封包過濾功能測試流程圖

(f) 測試結果：

- (1) 對於設定禁止接收之 N3 介面，gNB 拋棄收到的 GTP-U Echo Request 信令後，不會對 UPF 發送 GTP-U Echo Response。
- (2) 對於設定允許接收之 N3 介面，gNB 成功收到 GTP-U Echo Request 信令後，對 UPF 發送 GTP-U Echo Response 信令。

6.1.6.2 N2 介面的模糊測試(非必測項目)

(a) 測試依據：

參考 3GPP TS 33.511 [1] 之第 4.4 小節與 3GPP TS 33.117 [2] 之第 4.4.4 小節。

(b) 測試目的：

驗證 N2 介面能夠適當處理非預期的 NGAP 封包。

(c) 測試前提：

- (1) gNB 可成功與 AMF 模糊測試器建立 5G 連線。
- (2) 測試人員可擷取 NGAP 封包並分析其封包內容。

(d) 測試佈局：

見圖 48。

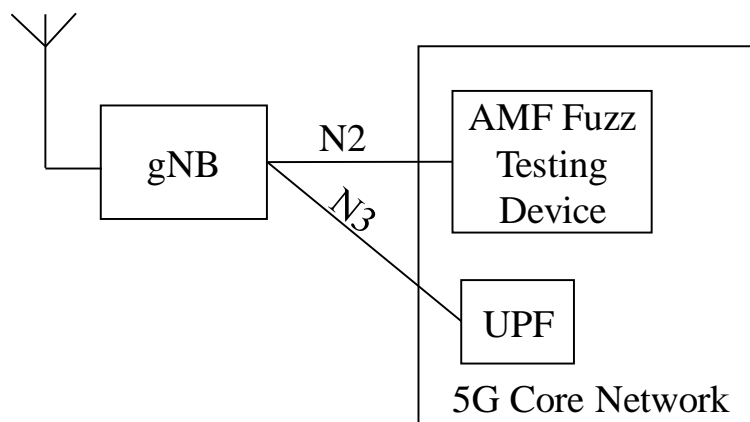


圖 48 N2 介面的模糊測試示意圖

(e) 測試步驟：

- (1) 開始擷取 NGAP 介面封包。
- (2) gNB 與 AMF 模糊測試器建立 NGAP 連線。
- (3) AMF 模糊測試器對 gNB 發送非預期的 NGAP 封包。
- (4) 停止擷取 NGAP 封包。
- (5) 透過 NGAP 封包，確認 gNB 是否捨棄非預期的 NGAP 封包亦或回覆 NGAP 封包錯誤。
- (6) 應用協定介面封包，gNB 重新與 AMF 模糊測試器建立 NGAP 連線。

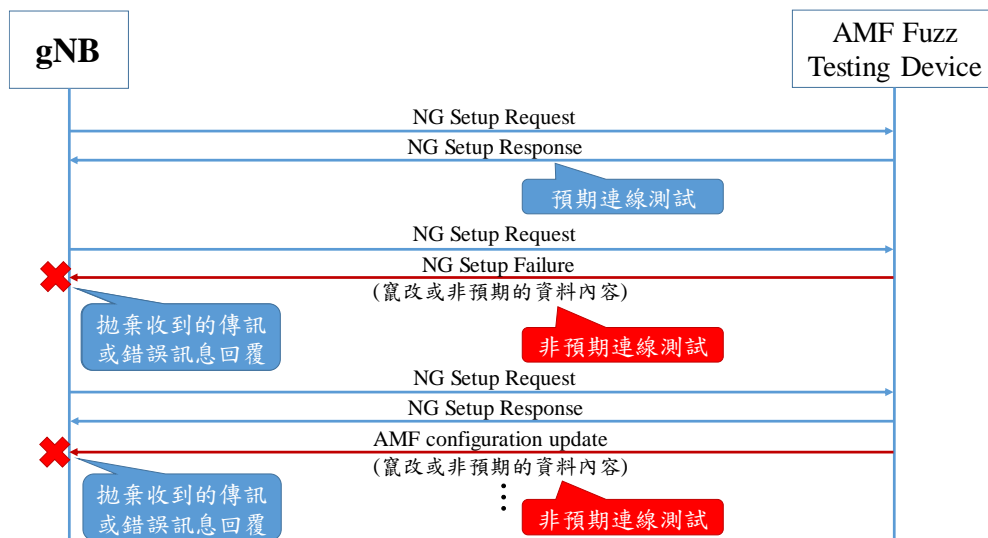


圖 49 N2 介面的模糊測試流程圖

(f) 測試結果：

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

6.1.6.3 N3 介面的模糊測試(非必測項目)

(a) 測試依據：

參考 3GPP TS 33.511 [1] 之第 4.4 小節與 3GPP TS 33.117 [2] 之第 4.4.4 小節。

(b) 測試目的：

驗證 N3 介面能夠適當處理非預期的 GTP-U 封包。

(c) 測試前提：

- (1) gNB 可成功與 AMF 建立 5G 連線。
- (2) 用戶終端與可成功透過 gNB 與 5GC 建立 NGAP 連線與用戶設備註冊。
- (3) AMF 可成功讓 gNB 與 UPF 模糊測試器建立 5G 連線。
- (4) 測試人員可擷取 GTP-U 封包，並分析通用 GTP-U 封包內容。

(d) 測試佈局：

見圖 50。

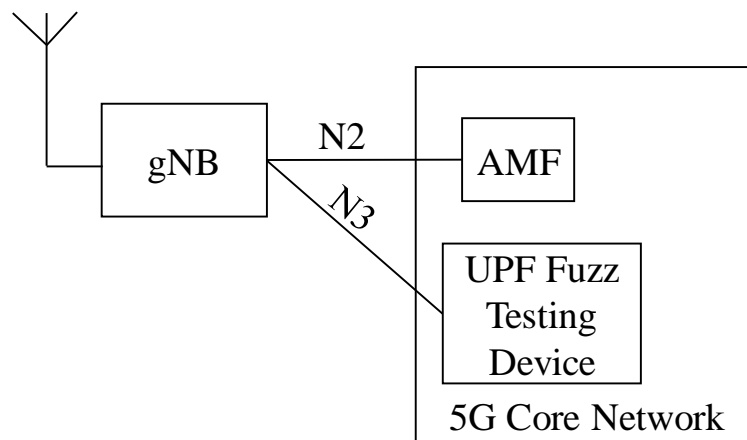


圖 50 N3 介面的模糊測試示意圖

(e) 測試步驟：

- (1) 開始擷取 GTP-U 介面封包。
- (2) gNB 與 UPF 模糊測試器建立 GTP-U 連線。
- (3) UPF 模糊測試器對 gNB 發送非預期的 GTP-U 封包。

- (4) 停止擷取 GTP-U 介面封包。
- (5) 透過用戶平面介面封包，確認 gNB 是否捨棄非預期的 GTP-U 封包亦或回覆 GTP-U 封包錯誤。
- (6) 透過 GTP-U 封包，gNB 重新與 UPF 模糊測試器建立 GTP-U 連線。

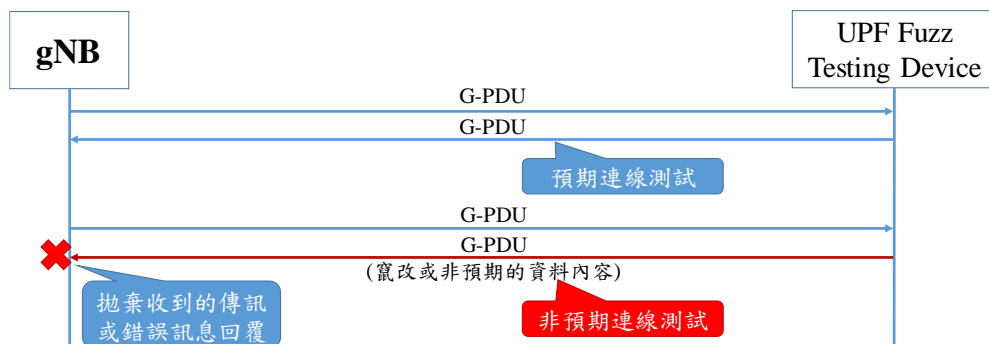


圖 51 N3 介面的模糊測試流程圖

(f) 測試結果：

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

6.1.6.4 Xn 介面的模糊測試(非必測項目)

(a) 測試依據：

參考 3GPP TS 33.511 [1] 之第 4.4 小節與 3GPP TS 33.117 [2] 之第 4.4.4 小節。

(b) 測試目的：

驗證 Xn 介面能夠適當處理非預期的 XnAP 封包。

(c) 測試前提：

- (1) gNB 可成功與 5GC 端建立 5G 連線。

- (2) gNB 模糊測試器可成功與 5GC 建立 5G 連線。
- (3) gNB 可成功透過 Xn 介面與 gNB 模糊測試器建立連線。
- (4) 測試人員可擷取 XnAP 封包並分析該封包內容。

(d) 測試佈局：

見圖 52。

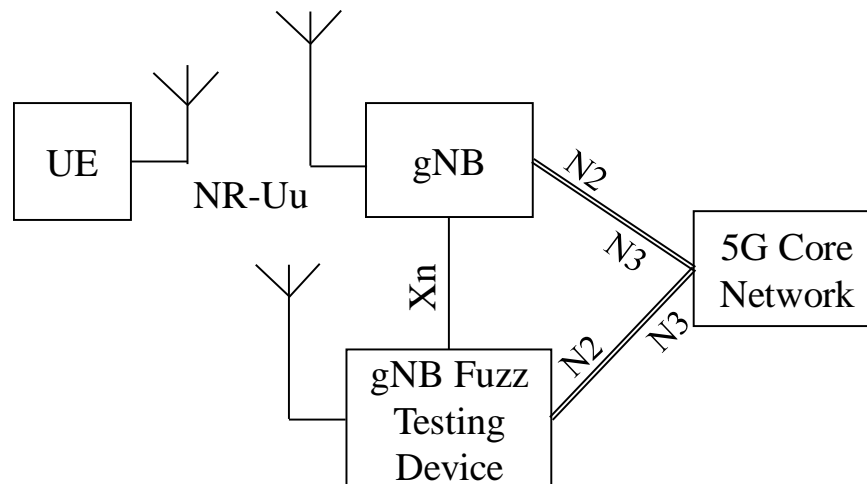


圖 52 Xn 介面的模糊測試示意圖

(e) 測試步驟：

- (1) 開始擷取下一代 XnAP 封包。
- (2) gNB 與 5GC 成功建立 5G 連線。
- (3) gNB 與 gNB 模糊測試器建立 Xn 應用協定連線。
- (4) gNB 模糊測試器對 gNB 發送非預期的 Xn 應用協定封包。
- (5) 停止擷取 XnAP 封包。
- (6) 透過 XnAP 封包，確認 gNB 是否捨棄非預期的 XnAP 封包亦或回覆 XnAP 封包錯誤。
- (7) gNB 重新與 gNB 模糊測試器建立 XnAP 連線。

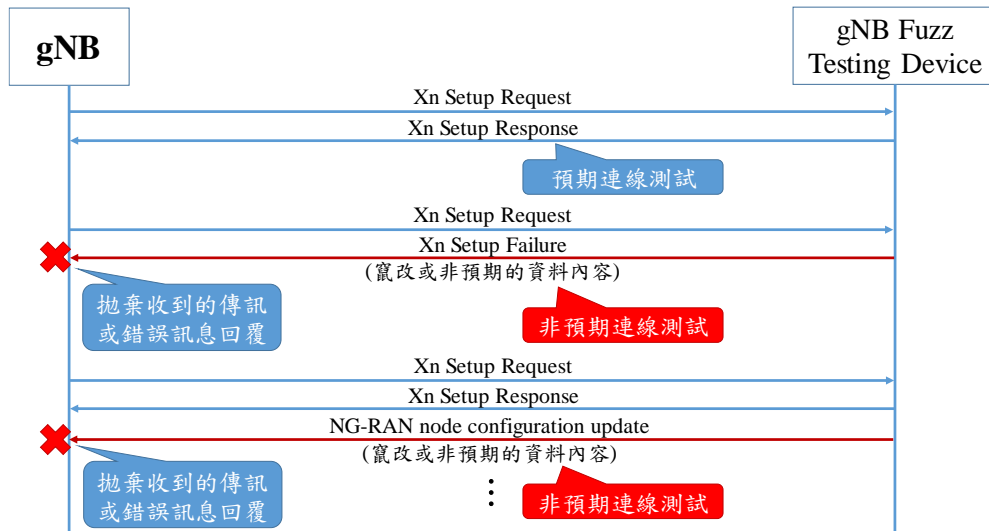


圖 53 Xn 介面的模糊測試流程圖

(f) 測試結果：

- (1) 根據步驟(6)和(7)，gNB 捨棄非預期的 XnAP 封包或回覆 XnAP 封包錯誤，並持續與建立 XnAP 連線。

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

(a) 測試依據：

參考 3GPP TS 33.511 [1] 與 3GPP TS 33.117 [3] 之第 4.2.3.2.2 小節。

(b) 測試目的：

從本地或遠端的營運管理與維護之命令語言解譯器(Command-Line Interface, CLI)或圖形化使用者介面(Graphical User Interface, GUI)、日誌訊息、警示、錯誤訊息、組態設定匯出檔確認並未存在敏感資料洩露風險。

(c) 測試前提：

gNB 供應商應提供以下書面資料作為審查與檢測依據：

- (1) 須提供所使用之系統功能書面資料。
- (2) 須提供所使用之系統登入帳號。

(d) 測試佈局：

見圖 54。

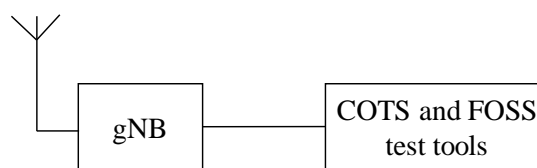


圖 54 系統功能造成敏感資料外洩測試示意圖

(e) 測試步驟：

- (1) 登入受測系統。
- (2) 檢視系統及應用服務組態設定檔是否包含敏感性資料。
- (3) 檢視本地或遠端的營運管理與維護之營運管理與維護 (OA&M) 命令語言解譯器或圖形化使用者介面是否包含敏感性資料。
- (4) 檢視日誌訊息是否包含敏感性資料。
- (5) 檢視錯誤訊息是否包含敏感性資料。

(f) 測試結果：

機密的系統內部敏感性資料，不應該被任何系統功能以明文 (plaintext) 的方式洩露。

6.2.1.2 韌體造成敏感資料外洩

(a) 測試依據：

參考 3GPP TS 33.511 [1] 與 3GPP TS 33.117 [3] 之第 4.2.3.2.3 小節。

附註：本測項參考 OWASP IoT Top Ten, 2014 (20) 之 I9 Insecure Software/Firmware 弱點之測試方式。

(b) 測試目的：

驗證 gNB 韌體並未含有敏感性資料外洩疑慮，包含預設的帳號密碼、預設的私鑰。

(c) 測試前提：

gNB 供應商應提供以下書面資料作為審查與檢測依據：

- (1) 須提供韌體檔案。
- (2) 須提供所使用之加密演算法書面資料作為審查依據。
- (3) 須提供所有相連伺服器之宣告。

(d) 測試佈局：

見圖 55。

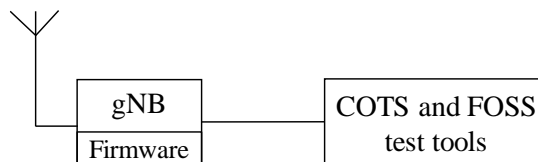


圖 55 韌體造成敏感資料外洩測試示意圖

(e) 測試步驟：

- (1) 使用韌體拆解功能之工具，對受測產品之韌體進行拆解。
- (2) 解析檔案系統之路徑目錄。
- (3) 確認私鑰是否可被擷取。
- (4) 檢查是否存在非公開帳號密碼資料。
- (5) 檢查是否存在非公開之電子郵件資料。
- (6) 檢查是否存在惡意或未宣告之網際網路協定位址資料。

(7) 檢查是否存在惡意或未宣告之全球資源定址器資料。

(f) 測試結果：

下述兩個合格標準擇一通過即可：

情境 1 合格標準：

(1) 韌體之加密演算法採用 FIPS 140-2 (21) 所核可之加密演算法。

情境 2 合格標準：

(1) 未加密之韌體檔案，通行碼保護機制採用 FIPS 140-2 所核可之雜湊函數。

(2) 未加密之韌體檔案，該私鑰不可被識別。

(3) 未加密之韌體檔案，不存在非公開帳號密碼資料

(4) 未加密之韌體檔案，不存在非公開之電子郵件資料。

(5) 未加密之韌體檔案，不存在惡意或未宣告之網際網路協定位址資料。

(6) 未加密之韌體檔案，不存在惡意或未宣告之 URL 資料。

6.2.1.3 確保敏感性資料進行加密處理再儲存

(a) 測試依據：

參考 3GPP TS 33.511 [1] 與 3GPP TS 33.117 [3] 之第 4.2.3.2.3 小節。

(b) 測試目的：

對於敏感性資料應採用適當且有效之加密技術，使資料不會以原來的形式呈現，達到保密的目的，並確保避免遭操作修改。

(c) 測試前提：

gNB 供應商應提供以下書面資料作為審查與檢測依據：

(1) 須提供系統敏感性資料儲存區域與存取操作書面資料。

(d) 測試佈局：

見圖 56。

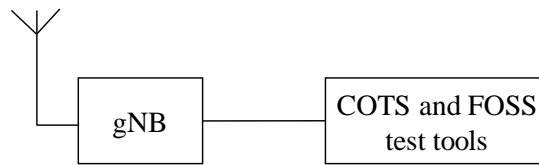


圖 56 確保敏感性資料進行加密處理再儲存測試示意圖

(e) 測試步驟：

- (1) 登入受測系統。
- (2) 檢視系統組態設定檔敏感性資料是否有加密。
- (3) 檢視日誌訊息敏感性資料是否有加密。
- (4) 檢視敏感性資料是否採用有效之加密技術，使資料以非明文(non-plaintext)顯示。

(f) 測試結果：

步驟(4)中，gNB 系統敏感性資料以非明文(non-plaintext)方式顯示。

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

(a) 測試依據：

參考 3GPP TS 33.511 [1] 與 3GPP TS 33.117 [3] 之第 4.3.4 小節。

(b) 測試目的：

針對網站介面，應確保網站伺服器不存在已知的高、中安全弱點，例如：注入攻擊(Injection)、跨框架腳本攻擊(Cross-Frame Scripting)、網站伺服器設定配置不當(Web Server Misconfiguration)等，以及 OWASP Top 10 所載之網站安全威脅弱點。

(c) 測試前提：

gNB 供應商應提供以下書面資料作為審查與檢測依據：

- (1) 提供網站伺服器管理權限之帳號密碼書面資料。

(d) 測試佈局：

見圖 59。

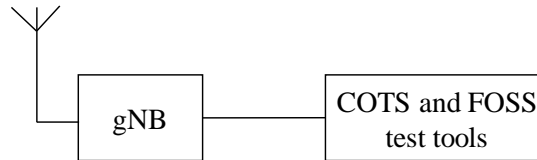


圖 59 網路應用系統安全弱點測試示意圖

(e) 測試步驟：

- (1) 使用埠掃描工具確認受測系統是否有網站伺服器運作。
- (2) 使用網站弱掃工具對網站伺服器進行檢測，如 Nessus、Acunetix。
- (3) 確認檢測報告是否含有中、高風險弱點存在。

(f) 測試結果：

步驟(3)中，安全檢測工具掃描 gNB 之結果不應存在中、高風險弱點。

6.2.2.2 系統使用之協定與服務採最小化設計

(a) 測試依據：

參考 3GPP TS 33.511 [1] 與 3GPP TS 33.117 [3] 之第 4.3.2.1 小節與第 4.3.3.1.2 小節。

(b) 測試目的：

實際維運階段預設只執行 gNB 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：

gNB 供應商應提供以下書面資料作為審查與檢測依據：

- (1) gNB 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 60。

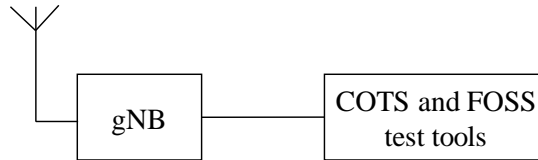


圖 60 系統使用之協定與服務採最小化設計測試示意圖

(e) 測試步驟：

- (1) 使用埠掃描工具檢測受測系統運行的服務列表。
- (2) 確認服務列表中的服務為 gNB 供應商實際維運階段所需協定與服務。
- (3) 重啟 gNB，重新執行步驟(1)至步驟(2)，確認服務列表中的服務為 gNB 供應商實際維運階段所需協定與服務。
- (4) 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 gNB 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。

6.2.2.3 網路傳輸過程使用加密技術確保資料安全

(a) 測試依據：

參考 3GPP TS 33.511 [1] 與 3GPP TS 33.117 [3] 之第 4.2.3.2.4 小節以及 3GPP TS 33.310 [5] 之附錄 E。

(b) 測試目的：

受測系統與外部設備網路傳輸過程須依實際維運需求，確保重要敏感資料有加密保護，不使用弱加密技術。

(c) 測試前提：

gNB 供應商應提供以下書面資料作為審查與檢測依據：

- (1) gNB 實際維運階段所需預設開啟之協定與服務用途列表。
- (2) 使用網路傳輸的加密演算法與安全協定名稱與版本。

(d) 測試佈局：

見圖 61。

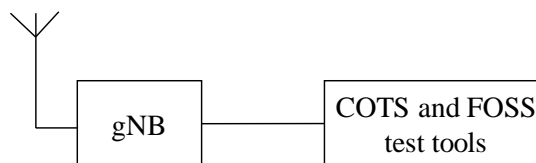


圖 61 網路傳輸過程使用加密技術確保資料安全測試示意圖

(e) 測試步驟：

- (1) 使用埠掃描 (Port Scan) 工具檢測受測系統運行的服務列表。
- (2) 側錄與保存步驟(2)網路傳輸過程間之通訊封包。
- (3) 確認傳輸重要敏感資料的服務中的有提供加密保護。
- (4) 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(3)中，gNB 系統敏感性資料以非明文 (Plain-Text) 方式顯示。

- (1) 若採用傳輸層安全性協定 (Transport Layer Security, TLS) 安全通道，則測試結果須符合 3GPP TS 33.310 [5] 之附錄 E。
- (2) 若採用 IKE 及 IPsec 安全通道，則測試結果須符合 3GPP TS 33.210 [4] 之第 5.3 小節及第 5.4 小節。

步驟(4)中，確認開啟之服務都有其合理與必要性。

6.2.3 身份鑑別與授權

6.2.3.1 禁止未經認證與授權使用系統各項功能

(a) 測試依據：

參考 3GPP TS 33.511 [1] 與 3GPP TS 33.117 [3] 之第 4.2.3.4.1.1 小節。

(b) 測試目的：

登入至系統包含管理介面、網路服務(SSH、SFTP、Web Service)，都須完成身分認證與授權機制後才可以使用系統各項功能。

(c) 測試前提：

gNB 供應商應提供以下書面資料作為審查與檢測依據：

- (1) gNB 實際維運階段所需協定與服務列表。
- (2) 提供所有可登入系統方式清單與使用說明文件。

(d) 測試佈局：

見圖 62。

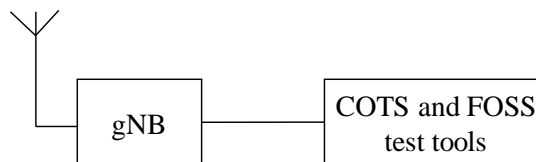


圖 62 禁止未經認證與授權使用系統各項功能測試示意圖

(e) 測試步驟：

- (1) 審查書面資料，確認已符合測試前提要求。
- (2) 測試人員根據書面使用說明資料嘗試登入系統，確認是否有完成認證與授權機制後，才可使用系統功能。

(f) 測試結果：

步驟(2)中，確認完成認證與授權機制後，才可登入系統與使用系統功能。

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

(a) 測試依據：

參考 3GPP TS 33.511 [1] 與 3GPP TS 33.117 [3] 之第 4.2.3.4.2.1 小節。

(b) 測試目的：

受測系統的使用者身分鑑別機制須至少帳號與一個身分鑑別因子，包含加密金鑰 (Cryptographic keys)、符記 (Token) 或密碼。

(c) 測試前提：

gNB 供應商應提供以下書面資料作為審查與檢測依據：

- (1) gNB 實際維運階段所需協定與服務列表。
- (2) 提供所有可登入系統方式清單與使用說明文件。

(d) 測試佈局：

見圖 63。

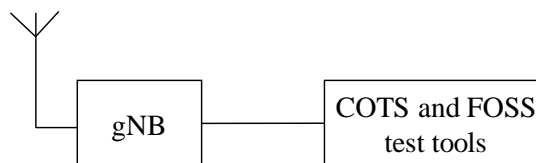


圖 63 帳號身分鑑別因子測試示意圖

(e) 測試步驟：

- (1) 審查書面資料，確認已符合測試前提要求。
- (2) 嘗試登入系統，確認是否有完成認證與授權機制後，才可使用系統功能。

(f) 測試結果：

步驟(1)中，確認完成認證與授權機制後，才可登入系統與使用限定功能。

6.2.3.3 系統預設帳號應可移除或設置停用

(a) 測試依據：

參考 3GPP TS 33.511 [1] 與 3GPP TS 33.117 [3] 之第 4.2.3.4.2.3 小節與第 4.2.3.4.2.2 小節。

(b) 測試目的：

預定義或預設帳號都應於初始化設定完成後給予移除或設置停用，避免預設使用已知帳號取得系統權限。

(c) 測試前提：

gNB 供應商應提供以下書面資料作為審查與檢測依據：

- (1) 提供 gNB 出廠預定義之帳號與密碼資料。
- (2) 提供帳號管理設定之操作文件。

(d) 測試佈局：

見圖 64。

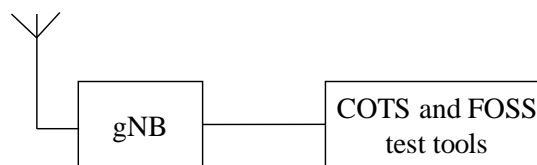


圖 64 系統預設帳號應可移除或設置停用測試示意圖

(e) 測試步驟：

- (1) 開啟受測系統登入畫面
- (2) 嘗試以預設定義帳號登入系統，確認是否會強制要求更改登入密碼。
- (3) 登入系統後，確認是否能移除或設置停用帳號。

(f) 測試結果：

步驟(2)中，確認系統要求強制更改登入密碼。若無強制更改密碼，則確認步驟(3)是否可以刪除或停用。如步驟(1)與步驟(2)無法完成，則至少要可將步驟(3)重置設定密碼複雜性才可符合判定標準。

6.2.3.4 系統應支援與設定不同組合之密碼複雜性規格

(a) 測試依據：

參考 3GPP TS 33.511 [1] 與 3GPP TS 33.117 [3] 之第 4.2.3.4.3.1 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：

gNB 供應商應提供以下書面資料作為審查與檢測依據：

- (1) 提供 gNB 密碼修改之操作文件。

(d) 測試佈局：

見圖 65。

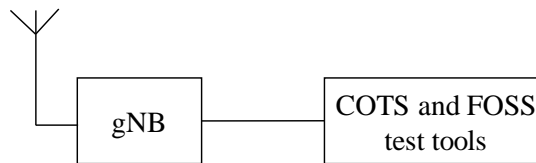


圖 65 密碼複雜性規格測試示意圖

(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。

6.2.3.5 密碼變更機制

(a) 測試依據：

參考 3GPP TS 33.511 [1] 與 3GPP TS 33.117 [3] 之第 4.2.3.4.3.2 小節。

(b) 測試目的：

系統應支援可提供隨時更改密碼之功能，並且系統預設密碼應於初次登入階段強制要求變更。

(c) 測試前提：

gNB 供應商應提供以下書面資料作為審查與檢測依據：

(1) 提供 gNB 密碼修改與相關設定之操作文件。

(d) 測試佈局：

見圖 66。

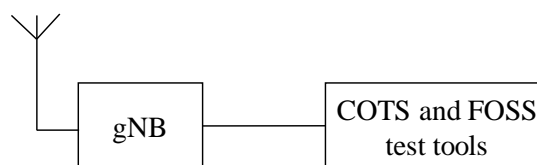


圖 66 密碼變更機制測試示意圖

(e) 測試步驟：

(1) 開啟受測系統登入畫面

(2) 使用系統內建預設密碼之帳號登入，測試人員觀察系統是否要求初次登入強制變更系統預設密碼。

(3) 使用正常帳號登入，確認是否能修改帳號密碼。

(f) 測試結果：

步驟(2)中，確認系統有強制要求初次登入變更系統預設密碼。步驟(3)中，確認密碼變更機制。

6.2.3.6 系統應具備暴力及字典攻擊的防護措施

(a) 測試依據：

參考 3GPP TS 33.511 [1] 與 3GPP TS 33.117 [3] 之第 4.2.3.4.3.3 小節。

(b) 測試目的：

當系統有提供管理介面或網路服務，應具備暴力字典攻擊的保護措施，例如：網頁介面設置驗證碼 (Completely Automated Public Turing test to tell Computers and Humans Apart, CAPTCHA) 功能、嘗試登入失敗次數限制與鎖定帳號時間或第三方網管軟體通知功能。

(c) 測試前提：

gNB 供應商應提供以下書面資料作為審查與檢測依據：

- (1) 提供 gNB 登入失敗次數限制功能操作說明。

(d) 測試佈局：

見圖 67。

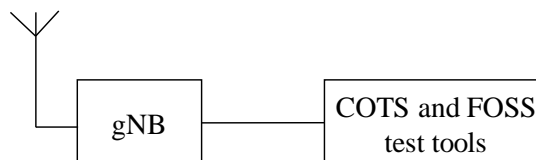


圖 67 系統應具備暴力及字典攻擊的防護措施測試示意圖

(e) 測試步驟：

- (1) 測試人員輸入不正確的密碼，確定系統是否於限制次數錯誤輸入後會鎖定帳號。
- (2) 測試人員使用測試工具嘗試進行暴力破解，確認測試工具是否可以正常的執行運作。
- (3) 使用正常帳號登入，確認是否能修改帳號密碼。

(f) 測試結果：

步驟(1)中，確認系統可鑑別錯誤次數輸入，鎖定帳號。

步驟(2)中，確認暴力破解工具無法執行。

6.2.3.7 密碼顯示遮罩

(a) 測試依據：

參考 3GPP TS 33.511 [1] 與 3GPP TS 33.117 [3] 之第 4.2.3.4.3.4 小節。

(b) 測試目的：

確認密碼輸入時不會原來的形式明文呈現，例如以*符號顯示目前字元，達到保密的目的，並確保避免遭操作修改。

(c) 測試前提：

無。

(d) 測試佈局：

見圖 68。

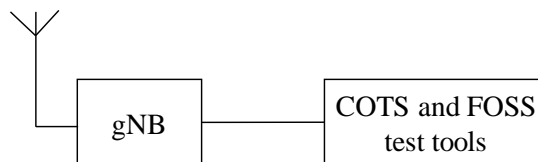


圖 68 密碼顯示遮罩測試示意圖

(e) 測試步驟：

(1) 開啟受測系統登入畫面

(2) 測試系統需輸入密碼之介面，觀測是否以遮罩形式呈現。

(f) 測試結果：

步驟(2)中，確認系統登入畫面之密碼顯示以遮罩形式呈現。

6.2.3.8 密碼連續輸入錯誤處理

(a) 測試依據：

參考 3GPP TS 33.511 [1] 與 3GPP TS 33.117 [3] 之第 4.2.3.4.5 小節。

(b) 測試目的：

系統應具備連續登入失敗處理機制，並可限制最大連續輸入失敗次數與強制鎖定可登入延遲時間或連續輸入錯誤通報機制。

(c) 測試前提：

gNB 供應商應提供以下書面資料作為審查與檢測依據：

(1) 提供 gNB 連續登入失敗處理機制之書面說明。

(d) 測試佈局：

見圖 69。

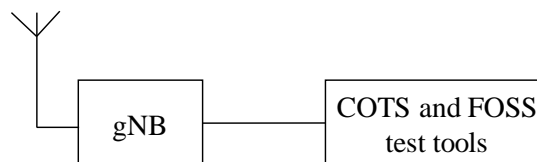


圖 69 密碼連續輸入錯誤處理測試示意圖

(e) 測試步驟：

(1) 根據書面資料設定連續登入失敗處理機制。

(2) 選擇特定帳號，並測試超出系統設定連續失敗登入最大次數，觀察系統是否有效啟用連續登入失敗處理機制，限制鎖定該帳號於特定時間後才可重新登入。

(f) 測試結果：

步驟(2)中，確認系統啟用連續登入失敗處理機制。

6.2.3.9 授權策略

(a) 測試依據：

參考 3GPP TS 33.511 [1] 與 3GPP TS 33.117 [3] 之第 4.2.3.4.6.1 小節。

(b) 測試目的：

gNB 系統應具備依不同帳號給予不同授權之設定機制，確保 gNB 之授權策略，針對特定資訊僅給予具備權限之帳號存取。

(c) 測試前提：

gNB 供應商應提供以下書面資料作為審查與檢測依據：

(1) 提供 gNB 授權策略功能與操作之書面說明。

(d) 測試佈局：

見圖 70。

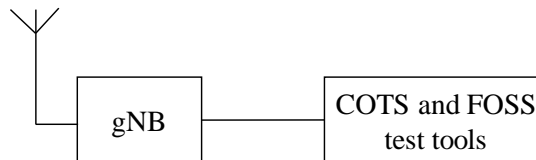


圖 70 授權策略測試示意圖

(e) 測試步驟：

(1) 嘗試操作不在權限範圍內之功能，確認是否可正常操作或系統有無提示警語。

(f) 測試結果：

步驟(1)中，確認系統確實對該帳號給予不同授權之設定，才可使用限定授權功能。

6.2.3.10 gNB 系統應支援基於角色之存取控制

(a) 測試依據：

參考 3GPP TS 33.511 [1] 與 3GPP TS 33.117 [3] 之第 4.2.3.4.1.2 小節、第 4.2.3.4.6.2 小節與第 4.2.4.2.2 小節。

(b) 測試目的：

gNB 系統應支援基於帳號角色之存取控制。使用一系列控制方式來確定帳號如何進行系統功能存取與故障管理維護。

(c) 測試前提：

gNB 供應商應提供以下書面資料作為審查與檢測依據：

- (1) 提供 gNB 基於角色存取控制功能操作說明。
- (2) 提供 gNB 可設定之所有權限清單說明。

(d) 測試佈局：

見圖 71。

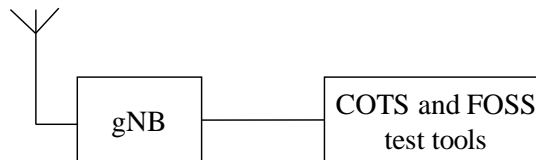


圖 71 gNB 系統應支援基於角色之存取控制測試示意圖

(e) 測試步驟：

- (1) 建立分配不同角色的帳號，並給予不同存取權限。
- (2) 使用不同的帳號測試不同角色可允許的功能操作。

(f) 測試結果：

步驟(2)中，確認系統可依不同角色帳號，設定不同權限使用限定授權功能。

6.2.3.11 登出功能是否有效

(a) 測試依據：

參考 3GPP TS 33.511 [1] 與 3GPP TS 33.117 [3] 之第 4.2.3.5.1 小節。

(b) 測試目的：

gNB 系統應支援登入之帳號可隨時登出之功能，並於登出階段提供是否登出系統之提醒畫面。

(c) 測試前提：

gNB 供應商應提供以下書面資料作為審查與檢測依據：

- (1) 提供 gNB 系統登出功能操作說明。

(d) 測試佈局：

見圖 72。

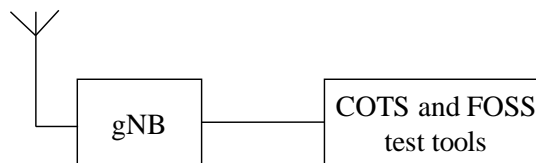


圖 72 登出功能是否有效測試示意圖

(e) 測試步驟：

- (1) 測試人員使用特定帳號登入系統。
- (2) 測試人員根據書面資料進行登出動作，確認系統是否顯示提醒畫面，並完成系統登出。

(f) 測試結果：

步驟(2)中，確認系統顯示登出提醒畫面與完成登出動作。

6.2.3.12 登入之權限控管

(a) 測試依據：

參考 3GPP TS 33.511 [1] 與 3GPP TS 33.117 [3] 之第 4.3.2.6 小節。

(b) 測試目的：

gNB 系統應限制最高管理權限帳號不可從遠端登入，降低被攻擊的風險。

(c) 測試前提：

gNB 供應商應提供以下書面資料作為審查與檢測依據：

- (1) 提供 gNB 系統如何遠端登入說明文件。

(2) 提供 gNB 如何限制最高管理權限帳號遠端登入之功能操作說明。

(d) 測試佈局：

見圖 73。

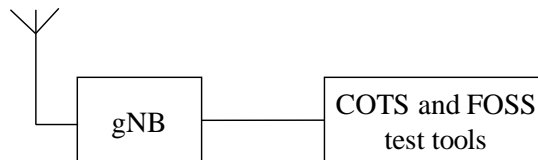


圖 73 登入之權限控管測試示意圖

(e) 測試步驟：

(1) 針對受測系統嘗試網路遠端登入 gNB 服務，並使用根權限或者最高權限的帳戶。

(f) 測試結果：

步驟(1)確認無法登入。

6.2.3.13 檔案系統存取權限控管

(a) 測試依據：

參考 3GPP TS 33.511 [1] 與 3GPP TS 33.117 [3] 之第 4.3.2.7 小節與第 4.3.3.1.6 小節。

(b) 測試目的：

gNB 系統應具備檔案系統存取權限控管機制，僅有授權之帳戶可修改作業系統層級之檔案、資料或系統檔案等。

(c) 測試前提：

gNB 供應商應提供以下書面資料作為審查與檢測依據：

(1) 提供 gNB 系統如何登入作業系統層級之操作介面。

(2) 提供 gNB 系統最高管理者帳號密碼。

(3) 提供 gNB 如何進行檔案系統存取權限控管機制之功能操作說明。

(d) 測試佈局：

見圖 74。

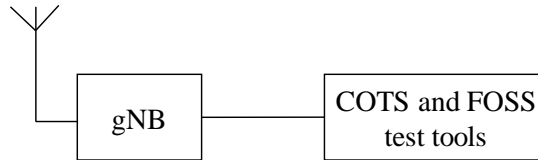


圖 74 檔案系統存取權限控管測試示意圖

(e) 測試步驟：

- (1) 使用最高權限帳號登入作業系統層級之操作介面。
- (2) 建立一個新的特定帳號。
- (3) 對此步驟(2)特定帳號行檔案系統存取權限設定。
- (4) 改以步驟(2)特定帳號登入作業系統層級之操作畫面，測試是否可對被限制之檔案系統進行存取動作。

(f) 測試結果：

步驟(4)確認步驟(2)特定帳號無法對檔案系統進行存取動作。

6.2.3.14 gNB 系統應支援操作逾時功能

(a) 測試依據：

參考 3GPP TS 33.511 [1] 與 3GPP TS 33.117 [3] 之第 4.2.3.5.2 小節。

(b) 測試目的：

gNB 系統應限制當帳戶操作逾時超出設定時間，系統即將該帳號給予強制登出。

(c) 測試前提：

gNB 供應商應提供以下書面資料作為審查與檢測依據：

- (1) 提供 gNB 系統設定逾時功能操作說明。

(2) 提供 gNB 系統內建逾時登出時間說明文件。

(d) 測試佈局：

見圖 75。

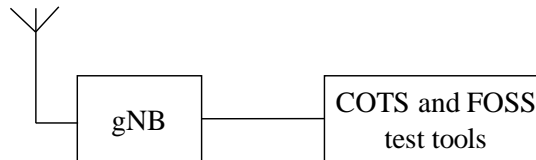


圖 75 gNB 系統應支援操作逾時功能測試示意圖

(e) 測試步驟：

(1) 登入受測系統，新建特定帳號，設定逾時登出時間。

(2) 以步驟(1)特定帳號登入系統，依所設定逾時登出時間進行操作閒置，確認系統是否依逾時設定對帳號進行強制登出。

(3) 若受測系統沒有逾時設定功能，測試人員使用預設帳號登入系統進行操作閒置，確認系統是否依逾時設定對帳號進行強制登出。

(f) 測試結果：

步驟(2)中，確認系統是否依逾時設定對帳號進行強制登出。若無執行步驟(2)，則步驟(3) 確認系統是否依逾時設定對預設帳號進行強制登出。

6.2.4 作業系統安全

6.2.4.1 日誌檔不能洩露個人資料

(a) 測試依據：

參考 3GPP TS 33.511 [1] 與 3GPP TS 33.117 [3] 之第 4.2.3.2.5 小節。

(b) 測試目的：

驗證受測系統之個人資料是否不會明文顯示於日誌檔中。

(c) 測試前提：

gNB 供應商應提供以下書面資料作為審查與檢測依據：

(1) 提供 gNB 系統日誌檔的位置說明。

(d) 測試佈局：

見圖 76。

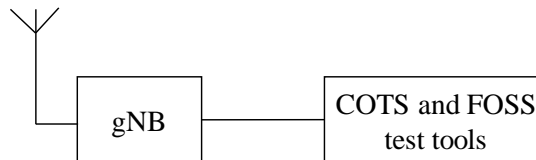


圖 76 日誌檔不能洩露個人資料測試示意圖

(e) 測試步驟：

(1) 檢視日誌檔明文顯示之位置，是否與聲明一致。

(2) 除個人日誌檔資料的位置外，檢視每一日誌檔中是否存在明文的個人資料。

(f) 測試結果：

確認該日誌檔中個人資料以明文顯示之正當性。

6.2.4.2 開機僅可透過合法的韌體

(a) 測試依據：

參考 3GPP TS 33.511 [1] 與 3GPP TS 33.117 [3] 之第 4.2.3.3.2 小節。

(b) 測試目的：

驗證受測系統是否只能由合法且未經竄改的韌體啟動。

(c) 測試前提：

gNB 供應商應提供以下書面資料作為審查與檢測依據：

(1) 提供 gNB 系統只能從限定記憶體裝置啟動之說明文件。

(d) 測試佈局：

見圖 77。

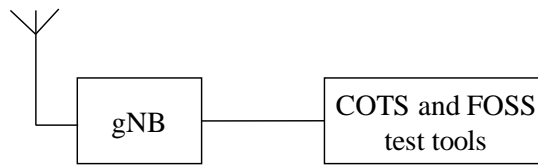


圖 77 開機僅可透過合法的韌體測試示意圖

(e) 測試步驟：

(1) 確認受測系統的啟動是否僅允許來自於合法且未經竄改的韌體。

(f) 測試結果：

韌體更新具有驗證機制，不接受竄改韌體啟動。

6.2.4.3 gNB 系統應具備軟體完整性自我檢測機制

(a) 測試依據：

參考 3GPP TS 33.511 [1] 與 3GPP TS 33.117 [3] 之第 4.2.3.3.5 小節。

(b) 測試目的：

受測系統應具備出廠預載軟體安裝時完整性檢測，驗證軟體是否已遭受修改。

(c) 測試前提：

gNB 供應商應提供以下書面資料作為審查與檢測依據：

(1) 提供 gNB 系統管理者權限。

(d) 測試佈局：

見圖 78。

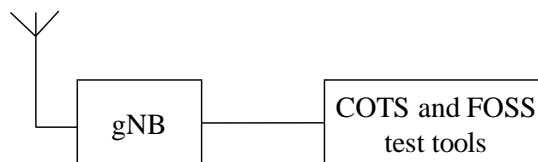


圖 78 軟體完整性自我檢測機制測試示意圖

(e) 測試步驟：

- (1) 以系統管理者權限登入系統。
- (2) 嘗試替換系統應用程式執行檔或系統網頁原始檔，驗證是否可被執行。

(f) 測試結果：

步驟(2)中，替換系統應用程式執行檔或網頁原始檔後，該軟體不可被執行。

6.2.4.4 系統應提供安全事件記錄功能

(a) 測試依據：

參考 3GPP TS 33.511 [1] 與 3GPP TS 33.117 [3] 之第 4.2.3.6.1 小節。

(b) 測試目的：

系統應提供不同事件類型之安全紀錄，包含登入失敗、管理者存取、管理者操作行為、設定變更、重新開機、關機、當機、網路介面狀態改變。

(c) 測試前提：

gNB 供應商應提供以下書面資料作為審查與檢測依據：

- (1) 提供如何存取、設定啟用安全事件紀錄操作文件。
- (2) 提供基站系統安全事件紀錄類型與格式說明文件。
- (3) 提供如何觸發每一個安全事件之操作文件。

(d) 測試佈局：

見圖 79。

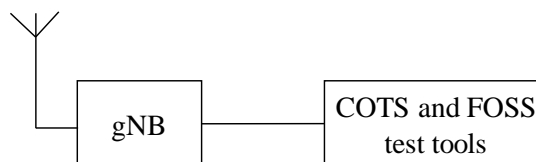


圖 79 系統應提供安全事件記錄功能測試示意圖

(e) 測試步驟：

(1) 測試人員依次觸發需求中列出的每個安全事件，確認系統有無記錄該事件。

(f) 測試結果：

步驟(1)中，確認系統是否依觸發不同安全事件而產生對應的紀錄。

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

(a) 測試依據：

參考 3GPP TS 33.511 [1] 與 3GPP TS 33.117 [3] 之第 4.2.3.6.2 小節。

(b) 測試目的：

gNB 系統應提供可將安全事件記錄功能傳輸備存至集中管理設備或其他外部系統設備，並於傳輸過程使用加密技術保護。

(c) 測試前提：

gNB 供應商應提供以下書面資料作為審查與檢測依據：

- (1) 提供安全事件紀錄傳輸至外部系統使用之標準協定文件。
- (2) 提供基站系統可支援傳輸安全事件紀錄之外部設備。
- (3) 提供如何觸發每一個安全事件之操作文件。

(d) 測試佈局：

見圖 80。

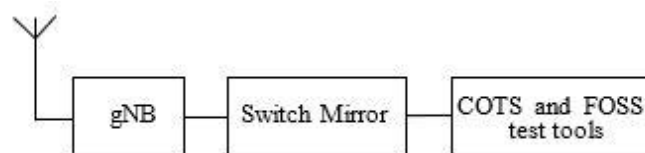


圖 80 安全事件記錄功能轉移備存至外部系統測試示意圖

(e) 測試步驟：

- (1) 觸發安全事件紀錄，將事件日誌傳送到外部系統。
- (2) 側錄與保存步驟(1)網路傳輸過程間之通訊封包。
- (3) 檢測集中式管理設備或外部系統是否儲存相關安全事件日誌。

(f) 測試結果：

- (1) 步驟(2)中，確認系統與外部系統之傳輸使用加密技術保護。
- (2) 步驟(3)確認集中式管理設備或外部系統確實紀錄來自受測系統傳送之相關安全事件紀錄。

6.2.4.6 gNB 系統的安全事件紀錄應有存取控制限制

(a) 測試依據：

參考 3GPP TS 33.511 [1] 與 3GPP TS 33.117 [3] 之第 4.2.3.6.3 小節。

(b) 測試目的：

gNB 系統之安全事件紀錄應僅有特定權限帳號可以存取。

(c) 測試前提：

無。

(d) 測試佈局：

見圖 81。

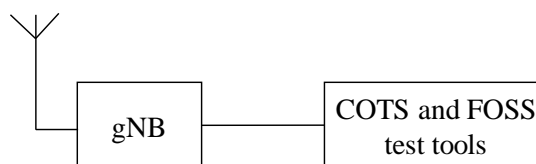


圖 81 安全事件紀錄應有存取控制限制測試示意圖

(e) 測試步驟：

(1) 使用具安全事件存取權限之帳號登入系統，確認是否可以存取安全事件日誌文件檔。

(2) 使用不具安全事件存取權限之帳號登入系統，確認是否可以存取安全事件日誌文件檔。

(f) 測試結果：

(1) 步驟(2)中，確認可以存取安全事件日誌文件檔。

(2) 步驟(3)，確認不可以存取安全事件日誌文件檔。

6.2.4.7 確保高權限的系統功能必須經過身分鑑別

(a) 測試依據：

參考 3GPP TS 33.511 [1] 與 3GPP TS 33.117 [3] 之第 4.2.4.1.2.1 小節。

(b) 測試目的：

驗證擁有特殊權限的系統功能是否經過認證與授權方可使用。

(c) 測試前提：

gNB 供應商應提供以下書面資料作為審查與檢測依據：

(1) 清單 A，以說明哪些系統函數可以取得高權限，以及其組態設定規則。例如：`sudo` 命令與相關設定檔案 `/etc/sudoers`。

(2) 清單 B，包括系統指令、圖形化使用者介面功能及檔案，這些即使較高權限只能執行特定的有限任務，在低特權用戶使用的情況下也是一樣。此列表還應包含：

i 設定這些指令和圖形化使用者介面功能。

ii 文件的擁有者和權限設定。

iii 這些指令、圖形化使用者介面功能及檔案的合理性。例如：擁有 SUID 與 SGID 權限的根用戶檔案。

(d) 測試佈局：

見圖 82。

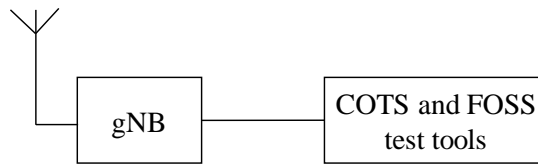


圖 82 確保高權限的系統功能必須經過身分鑑別測試示意圖

(e) 測試步驟：

- (1) 測試者須判斷清單 A 中內容的合理性外，並驗證是否使用都要經過身分認證。
- (2) 測試者須判斷清單 B 中內容描述的正确性及合理性外，並驗證是否使用都要經過身分認證。
- (3) 測試人員驗證列表“B”中的文件項目對擁有者之外的其他任何人都沒有寫入權限。
- (4) 實際執行列表 B 所描述的內容。

(f) 測試結果：

- (1) 產品不允許使用者透過另一個使用者帳戶，在沒有重新認證的情況下，取得系統管理者權限。
- (2) 功能及檔案的執行權限，必須與清單的一致。

6.2.4.8 可卸除儲存媒體禁止啟用自動播放功能

(a) 測試依據：

參考 3GPP TS 33.511 [1] 與 3GPP TS 33.117 [3] 之第 4.3.3.1.3 小節。

(b) 測試目的：

驗證當 gNB 被接入卸除式媒體(如：USB)時，是否會自動執行應用程式。

(c) 測試前提：

無。

(d) 測試佈局：

見圖 83。

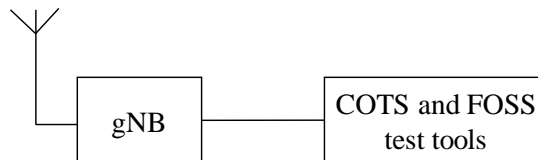


圖 83 可卸除儲存媒體禁止啟用自動播放功能測試示意圖

(e) 測試步驟：

(1) 測試者插入卸除式媒體至 gNB。

(f) 測試結果：

gNB 在插入卸除式媒體時，不會自動啟動應用程式。

6.2.4.9 作業系統及網路服務安全

(a) 測試依據：

參考 3GPP TS 33.511 [1] 與 3GPP TS 33.117 [3] 之第 4.2.4 小節、第 4.3.3 小節、第 4.4.2 小節與第 4.4.3 小節。

(b) 測試目的：

系統本身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：

無。

(d) 測試佈局：

見圖 84。

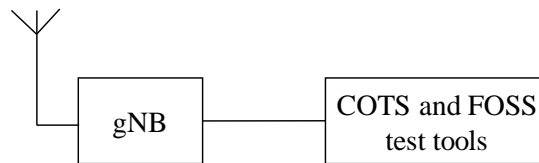


圖 84 作業系統及網路服務安全測試示意圖

(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 gNB 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(23) 評分為 7 分以上之資安漏洞。

(f) 測試結果：

作業系統與網路服務不存在 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。

附錄 A (參考) gNB 資安測試標準對應表

本測試規範參考第三代合作夥伴計畫所制定之「3GPP TS 33.511 Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class」[1]、
「3GPP TS 33.513-g10 5G Security Assurance Specification (SCAS); User Plane Function (UPF)」[2]與「3GPP TS 33.117 Catalogue of general security assurance requirement」[3]的資安需求 (security requirement)，針對 gNB 訂定資安測試規範之實施細節，其中資安需求的章節與本測試規範的章節對應關係如表 A.1 與表 A.2 以及表 A.3 所示。

表 A.1 3GPP TS 33.511 之第 4.2.2 節與本資安測試規範章節對應表

標準章節	測試項目	本資安測試規範章節
4.2.2.1.1	無線資源控制信令的完整性保護	6.1.1.1
4.2.2.1.2	用戶設備和基地臺間的用戶數據資料完整性保護	6.1.2.1
4.2.2.1.4	無線資源控制完整性檢查失敗	6.1.1.2
4.2.2.1.5	用戶平面完整性檢查失敗	6.1.2.2
4.2.2.1.6	無線資源控制信令加密	6.1.1.3
4.2.2.1.7	用戶設備和基地臺間的用戶平面資料加密	6.1.2.3
4.2.2.1.8	用戶設備與基地臺間的用戶數據資料重播攻擊保護	6.1.2.4
4.2.2.1.9	無線資源控制信令重播攻擊保護	6.1.1.4
4.2.2.1.10	基於連結管理功能傳送的安全策略對用戶平面資料進行加密	6.1.2.5
4.2.2.1.11	基於連結管理功能傳送的安全策略對用戶平面資料進行完整性保護	6.1.2.6
4.2.2.1.12	gNB 存取層加密和完整性演算法優先順序	6.1.3.1
4.2.2.1.13	gNB 金鑰更新	6.1.3.3
4.2.2.1.14	防範 Xn 介面交遞中的降階攻擊	6.1.4.1
4.2.2.1.15	於 5G 基地變更時存取層安全演算法選擇	6.1.4.2
4.2.2.1.16	控制平面資料在 N2 與 Xn 介面的機密性保護	6.1.5.1 6.1.5.3
4.2.2.1.17	控制平面資料在 N2 與 Xn 介面的完整性保護	6.1.5.4 6.1.5.6
4.2.2.1.18	雙連線的 gNB 金鑰更新	6.1.3.4 6.2.3.5

表 A.2 3GPP TS 33.513 之第 4.2.2 節與本資安測試規範章節對應表

標準章節	測試項目	本資安測試規範章節
4.2.2.1	通過 N3 介面傳輸之用戶數據的機密性保護	6.1.5.2
4.2.2.2	通過 N3 介面傳輸之用戶數據的完整性保護	6.1.5.5
4.2.2.3	通過 N3 介面傳輸之用戶數據的重播保護	

表 A.3 3GPP TS 33.511/TS 33.117 之第 4.2.3 節至第 4.4.4 節與本資安測試規範章節對應表

分類	標準章節	測試項目	本資安測試規範章節	
保護數據和資訊	4.2.3.2.2	未經授權的檢視	6.2.1.1	
	4.2.3.2.3	保護存儲中的數據和資訊	6.2.1.2 6.2.1.3	
	4.2.3.2.4	保護傳輸中的數據和資訊	6.2.2.3	
	4.2.3.2.5	記錄訪問個人數據的事件	6.2.4.1	
保護可用性和完整性	4.2.3.3.1	系統處理過載的情況		
	4.2.3.3.2	僅從預設的存儲設備開機	6.2.4.2	
	4.2.3.3.3	系統處理過度過載的情況		
	4.2.3.3.4	系統針對非預期輸入的強健性		
	4.2.3.3.5	網路產品軟體的完整性驗證	6.2.4.3	
認證與授權	認證政策	4.2.3.4.1.1	未經成功認證和授權，不得使用或訪問系統功能	6.2.3.1
		4.2.3.4.1.2	網路產品應使用明確標識的用戶帳戶	6.2.3.10
	認證屬性	4.2.3.4.2.1	至少透過一個身份驗證屬性保護帳戶	6.2.3.2
		4.2.3.4.2.2	預設帳戶應刪除或禁用	6.2.3.3
		4.2.3.4.2.3	預設認證屬性應刪除或禁用	6.2.3.3
	密碼政策	4.2.3.4.3.1	密碼複雜度規則	6.2.3.4
		4.2.3.4.3.2	密碼變更	6.2.3.5
		4.2.3.4.3.3	防止暴力和字典攻擊	6.2.3.6
		4.2.3.4.3.4	隱藏密碼顯示	6.2.3.7
	特定身份驗證案例	4.2.3.4.4.1	網路產品管理和維護界面	
	因應連續登錄失敗	4.2.3.4.5	有關連續嘗試登錄失敗的策略	6.2.3.8
	控制授權和訪問	4.2.3.4.6.1	授權政策	6.2.3.9
4.2.3.4.6.2		基於角色的訪問控制	6.2.3.10	
保護會話	4.2.3.5.1	保護會話 - 登出功能	6.2.3.11	

	4.2.3.5.2	保護會話 - 不活動逾時	6.2.3.14		
記錄	4.2.3.6.1	安全事件記錄	6.2.4.4		
	4.2.3.6.2	日誌傳輸到集中存儲	6.2.4.5		
	4.2.3.6.3	保護安全事件日誌文件	6.2.4.6		
作業系統	可用性和完整性	4.2.4.1.1.1	動態增長的內容不應影響系統功能	6.2.4.9	
		4.2.4.1.1.2	處理網際網路控制訊息協定第四版 (Internet Control Message Protocol version 4, ICMPv4) 和網際網路控制訊息協定第六版 (ICMPv6) 封包	6.2.4.9	
		4.2.4.1.1.3	不處理具有非必選或延伸標頭的網際網路協定 (Internet protocol, IP) 封包	6.2.4.9	
	認證與授權	4.2.4.1.2.1	僅允許經過身份驗證的特權升級	6.2.4.7	
	UNIX®	4.2.4.2.1	通則	6.2.4.9	
		4.2.4.2.2	系統帳號識別	6.2.3.10	
	安全強化 (hardening)	4.3.3.1.1	因應網際網路協定 (IP) 來源位置欺騙	6.2.4.9	
		4.3.3.1.2	核心網路功能最小化	6.2.2.2	
		4.3.3.1.3	沒有自動開啟可移除式媒體	6.2.4.8	
		4.3.3.1.4	預防請求洪水 (Syn Flood)	6.2.4.9	
		4.3.3.1.5	防止緩衝器溢位的保護機制	6.2.4.9	
		4.3.3.1.6	限制安裝外部檔案系統	6.2.3.13	
	網頁伺服器	網頁安全	4.2.5.1	超文本傳輸安全協定 (HyperText Transfer Protocol Secure, HTTPS)	6.2.2.1
			4.2.5.2.1	網頁伺服器日誌記錄	6.2.2.1
			4.2.5.3	用戶會話	6.2.2.1
			4.2.5.4	輸入驗證	6.2.2.1
安全強化 (hardening)		4.3.4.1	通則	6.2.2.1	
		4.3.4.2	網頁伺服器沒有系統特權	6.2.2.1	
		4.3.4.3	未使用的超文本傳輸協定 (HyperText Transfer Protocol, HTTP) 的方法 (methods) 應被停用	6.2.2.1	
		4.3.4.4	應停用不需要的附加元件	6.2.2.1	
		4.3.4.5	沒有通過共同閘道介面 (Common Gateway Interface, CGI) 或其他伺服器端腳本編寫的編譯器、解釋器或殼層 (Shell)	6.2.2.1	
		4.3.4.6	沒有用於上傳的共同閘道介面 (CGI) 或其他腳本	6.2.2.1	
		4.3.4.7	不使用伺服器端包含變數值 (Server Side Includes, SSI) 執行系統命令	6.2.2.1	
		4.3.4.8	管理網頁伺服器的權限僅應授予網頁伺服器的所有者或具有系統特權的用戶	6.2.2.1	
		4.3.4.9	應刪除預設的內容	6.2.2.1	
		4.3.4.10	沒有目錄列表/目錄瀏覽	6.2.2.1	
		4.3.4.11	應最小化超文本傳輸協定 (HTTP) 標頭中有關網頁伺服器的資訊	6.2.2.1	

		4.3.4.12	應刪除網頁伺服器中的錯誤資訊頁面	6.2.2.1
		4.3.4.13	應刪除不需要的檔案類型或腳本映射	6.2.2.1
		4.3.4.14	網頁伺服器僅交付必要的檔案	6.2.2.1
		4.3.4.15	僅在共同開道介面 (CGI) 與腳本目錄中具有執行權限	6.2.2.1
網路裝置	保護可用性和完整性	4.2.6.2.1	封包過濾	
		4.2.6.2.2	發送到網路設備的變造封包不應導致可用性降低	
		4.2.6.2.4	通用封包無線服務隧道協定-用戶平面 (GTP-U) 封包過濾	6.1.6.1
	安全強化	4.3.5.1	流量分離	
安全強化的技術準則		4.3.2.1	沒有不必要或不安全的服務與協議	6.2.2.2
		4.3.2.2	網路產品應限制服務的可達性	
		4.3.2.3	卸載或不得安裝未使用的軟體	
		4.3.2.4	未使用的網路產品軟硬體功能應被停用	
		4.3.2.5	網路產品不得包含供應商、生產商或開發人員不再支援的軟硬體元件。	
		4.3.2.6	限制特權用戶從遠端登錄	6.2.3.12
		4.3.2.7	檔案系統需要授權特權	6.2.3.13
基本弱點		4.4.2	通訊埠掃描	6.2.4.9
		4.4.3	弱點掃描	6.2.4.9
		4.4.4	強健性模糊測試	6.1.6.2
				6.1.6.3
				6.1.6.4

附錄 B (參考) 議題風險評估表

(a) 議題描述

國際網路安全協定 (IPsec) 功能未開啟

(b) 議題無法修改原因

內網、機房防護足夠、開啟 tunneling 會拖累速度

(c) 風險綜合評估結果

經列舉 3 項風險，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	傳輸資料被竊取	傳輸時未加密，導致可能遭偷聽竊取	gNB	XX 資料洩漏	(1)在 XXX 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							
3							

注*：應對措施已足以將風險降至極低程度

參考資料

- (1) Flaws in 4G, 5G networks could let hackers intercept calls, track location
(<https://www.purdue.edu/newsroom/releases/2019/Q1/flaws-in-4g,-5g-networks-could-let-hackers-intercept-calls,-track-location.html>)
- (2) GSMA Doc CVD-2019-0024
(https://www.3gpp.org/ftp/TSG_SA/WG3_SECURITY/TSGS3_95Bis_Sapporo/Docs/S3-192266.zip)
- (3) The Prague Proposals : The Chairman Statement on cyber security of communication networks in a globally digitalized world, Prague 5G Security Conference
- (4) 我國 5G 頻譜政策與專網發展, 行政院科技會報辦公室, 臺灣
- (5) 第五代行動通信系統資通安全維護計畫參考框架, 國家通訊傳播委員會, 臺灣
- (6) Cybersecurity Framework, NIST, USA (<https://www.nist.gov/cyberframework>)
- (7) EU coordinated risk assessment of the cybersecurity of 5G networks, NIS Cooperation Group, EU (9 October 2019)
(https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132)
- (8) 3GPP TS 22.261-i61 Service requirements for the 5G system; Stage 1 (Release 18)
(https://www.3gpp.org/ftp/Specs/archive/22_series/22.261/22261-i61.zip)
- (9) 3GPP TS 23.501-h50 System architecture for the 5G System (5GS); Stage 2 (Release 17)
(https://www.3gpp.org/ftp/Specs/archive/23_series/23.501/23501-h50.zip)
- (10) 3GPP TR 21.905-h10 Vocabulary for 3GPP Specifications (Release 17)
(https://www.3gpp.org/ftp/Specs/archive/21_series/21.905/21905-h10.zip)
- (11) 3GPP TS 38.300-h00 NR; NR and NG-RAN Overall Description; Stage 2 (Release 17)
(https://www.3gpp.org/ftp/Specs/archive/38_series/38.300/38300-h00.zip)
- (12) 3GPP TR 36.932-h00 Scenarios and requirements for small cell enhancements for E-UTRA and E-UTRAN (Release 17)
(https://www.3gpp.org/ftp/Specs/archive/36_series/36.932/36932-h00.zip)
- (13) Small cell definition, Small Cell Forum (<https://www.smallcellforum.org/what-is-a-small-cell/>)
- (14) 3GPP TS 38.413-h10 NG Application Protocol (NGAP) (Release 17)
(https://www.3gpp.org/ftp/Specs/archive/38_series/38.413/38413-h10.zip)

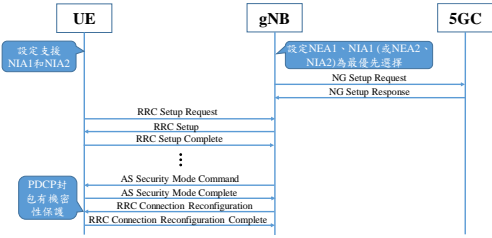
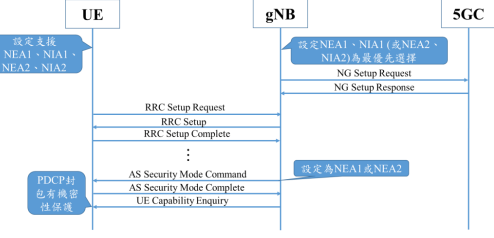
- (15) 3GPP TS 38.424-h00 NG-RAN; Xn data transport (Release 17)
(https://www.3gpp.org/ftp/Specs/archive/38_series/38.424/38424-h00.zip)
- (16) 3GPP TS 29.281-h30 General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U) (Release 17) (https://www.3gpp.org/ftp/Specs/archive/29_series/29.281/29281-h30.zip)
- (17) 3GPP TR 38.913-h00 Next Generation Access Technologies; (Release 17)
(https://www.3gpp.org/ftp/Specs/archive/38_series/38.913/38913-h00.zip)
- (18) IETF RFC 2408 Internet Security Association and Key Management Protocol
(<https://datatracker.ietf.org/doc/html/rfc2408>)
- (19) IETF RFC 2409 The Internet Key Exchange (IKE)
(<https://datatracker.ietf.org/doc/html/rfc2409>)
- (20) Open Web Application Security Project (OWASP) Internet of Things (IoT) Top Ten, 2014
(https://www.owasp.org/images/7/71/Internet_of_Things_Top_Ten_2014-OWASP.pdf)
- (21) NIST FIPS PUB 140-2, Security Requirements for Cryptographic Modules
(<https://csrc.nist.gov/publications/detail/fips/140/2/final>)
- (22) 3GPP TR 33.820-830, Security of H(e)NB (Release 8)
(https://www.3gpp.org/ftp/Specs/archive/33_series/33.820/33820-830.zip)
- (23) Common Vulnerability Scoring System (CVSS) v3.1 Specification, First
(<https://www.first.org/cvss/specification-document>)

版本修改紀錄

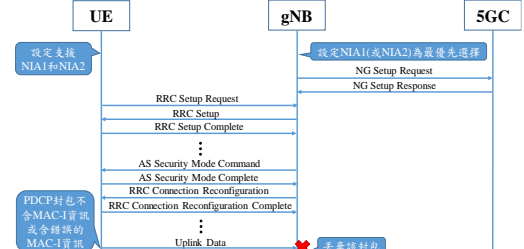
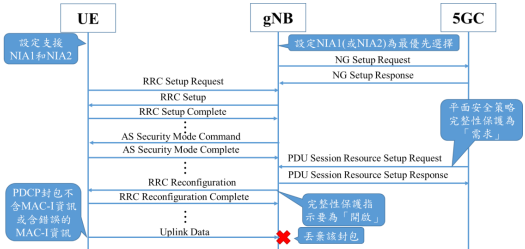
版本	時間	摘要
v1.0	2021/01/28	v1.0 出版
v2.0	2022/10/20	v2.0 出版

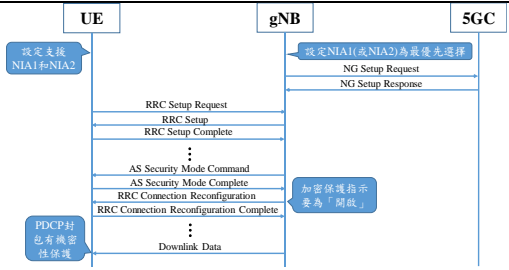
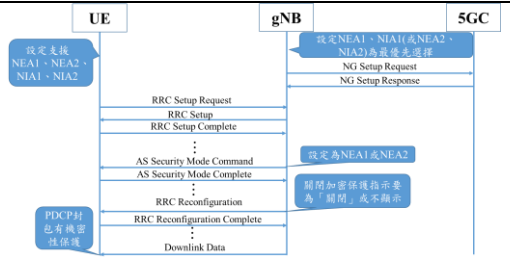
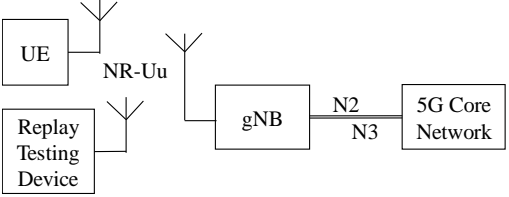
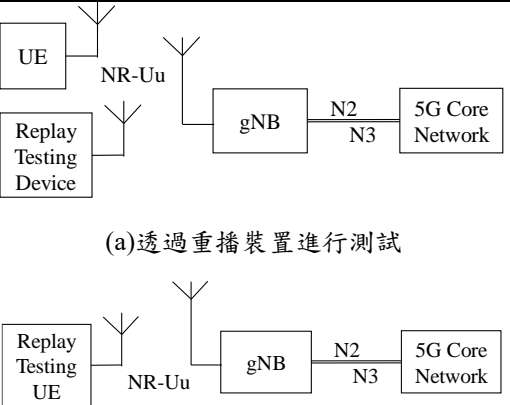
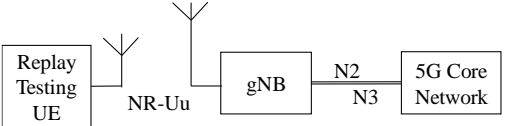
修改紀錄表

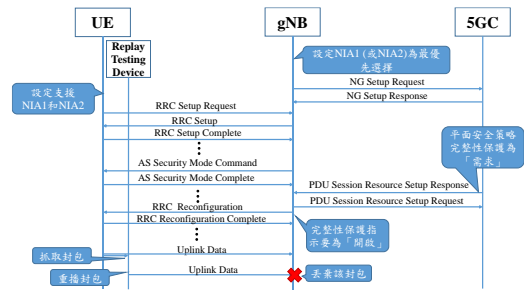
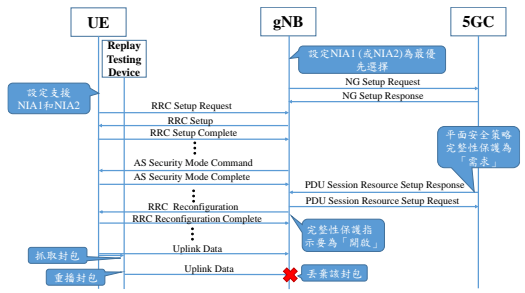
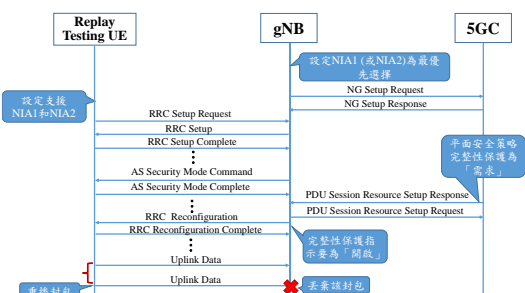
章節	內容	
	修訂前	修訂後
6.1.1.1	<p>(c) 測試前提：</p> <p>(1) 用戶設備及 gNB 可進行完整性安全演算法設定。</p> <p>(2) 用戶設備、gNB 及核心網路端可成功建立 5G 連線。</p>	<p>(c) 測試前提：</p> <p>(1) 用戶設備及 gNB 間可以進行完整性安全演算法設定。</p> <p>(2) 用戶設備、gNB 及 5GC 間可以成功建立 5G 連線。</p>
6.1.1.1	<p>(e) 測試步驟：</p> <p>(4) gNB 與 5GC 建立 NGAP 連線，並確認用戶設備註冊上核心網路。</p> <p>(5) 停止擷取 NGAP 介面封包。</p>	<p>(e) 測試步驟：</p> <p>(4) 確認 gNB 與 5GC 間建立 NGAP 連線，且用戶設備註冊上 5GC。</p> <p>(5) 停止擷取 NG-RAN 介面封包。</p>
6.1.1.1	<p>圖 3 RRC 信令的完整性保護測試流程圖</p>	<p>圖 3 RRC 信令的完整性保護測試流程圖</p>
6.1.1.2	<p>(c) 測試前提：</p> <p>(1) 用戶設備及 gNB 可進行完整性安全演算法設定。</p> <p>(2) 用戶設備、gNB 及核心網路端可成功建立 5G 連線。</p> <p>(3) 用戶設備可以修改 RRC 信令對應的 PDCP 層的訊息完整性鑑別碼。</p> <p>(4) 測試人員可擷取 RG-RAN 介面封包，並分析 RRC 封包之 PDCP 層的內容。</p>	<p>(c) 測試前提：</p> <p>(1) 用戶設備及 gNB 間可以進行完整性安全演算法設定。</p> <p>(2) 用戶設備、gNB 及 5GC 間可以成功建立 5G 連線。</p> <p>(3) 用戶設備可以修改 RRC 信令對應之 PDCP 層的訊息完整性鑑別碼。</p> <p>(4) 測試人員可擷取 NG-RAN 介面封包，並分析 RRC 封包之 PDCP 層的內容。</p>
6.1.1.2	<p>(e) 測試步驟：</p> <p>(4) gNB 與 5GC 建立 NGAP 連線，並進行用戶設備註冊。</p> <p>(5) 從 NG-RAN 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 gNB 的 RRC 信令封包。而選定的 RRC 信令帶有不含訊息完整性鑑別碼資訊或含錯誤的訊息完整性鑑別碼資訊在對應的 PDCP 層的訊息。</p> <p>(7) 透過 NG-RAN 介面封包，確認 gNB 是否檢查完整性鑑別碼之正確性。</p>	<p>(e) 測試步驟：</p> <p>(4) 確認 gNB 與 5GC 間建立 NGAP 連線，且用戶設備註冊。</p> <p>(5) 從 NG-RAN 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 gNB 的 RRC 信令封包。而選定的 RRC 信令之 PDCP 層的訊息帶有不含訊息完整性鑑別碼資訊或含錯誤的訊息完整性鑑別碼資訊。</p> <p>(7) 透過 NG-RAN 介面封包，確認 gNB 是否檢查完整性鑑別碼之正確性。</p>

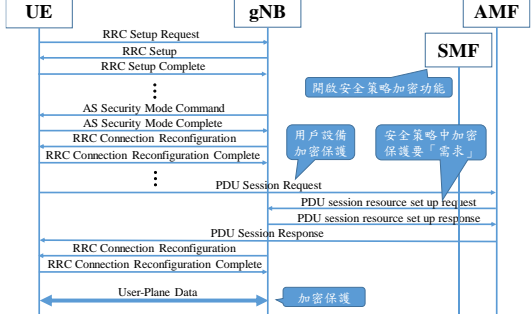
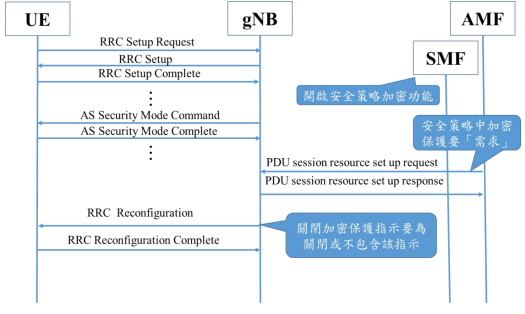
6.1.1.2	<p>(c) 測試前提：</p> <p>(1) 用戶設備及 gNB 可進行機密和完整性安全演算法設定。</p> <p>(2) 用戶設備、gNB 及核心網路端可成功建立 5G 連線。</p>	<p>(c) 測試前提：</p> <p>(1) 用戶設備及 gNB 間可以進行機密和完整性安全演算法設定。</p> <p>(2) 用戶設備、gNB 及 5GC 間可以成功建立 5G 連線。</p>
6.1.1.3	<p>(e) 測試步驟：</p> <p>(4) gNB 與 5GC 建立 NGAP 連線，並確認用戶設備註冊上核心網路。</p> <p>(7) 透過 NG-RAN 介面封包，在完成 RRC 信令安全驗證程序後，確認用戶設備和 gNB 間的 RRC 信令是否在對應的 PDCP 層中的訊息進行加密。</p>	<p>(e) 測試步驟：</p> <p>(4) 確認 gNB 與 5GC 間建立 NGAP 連線，且用戶設備註冊上 5GC。</p> <p>(7) 透過 NG-RAN 介面封包，在完成 RRC 信令安全驗證程序後，確認用戶設備和 gNB 間的 RRC 信令是否在對應之 PDCP 層中的訊息進行加密。</p>
6.1.1.3	 <p>圖 7 RRC 信令加密測試流程圖</p>	 <p>圖 7 RRC 信令加密測試流程圖</p>
6.1.1.4	<p>(c) 測試前提：</p> <p>(1) 用戶設備及 gNB 可進行機密和完整性安全演算法設定。</p> <p>(2) 用戶設備、gNB 及核心網路端可成功建立 5G 連線。</p>	<p>(c) 測試前提：</p> <p>(1) 用戶設備及 gNB 間可以進行機密和完整性安全演算法設定。</p> <p>(2) 用戶設備、gNB 及 5GC 間可以成功建立 5G 連線。</p>
6.1.1.4	<p>(e) 測試步驟：</p> <p>(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</p> <p>(2) 在 gNB 端設定 NEA1、NIA1 機密和完整性安全演算法為最優先選擇。</p> <p>(4) gNB 與 5GC 建立 NGAP 連線，並讓用戶設備註冊 5G 網路。</p> <p>(6) 從擷取的 NG-RAN 介面資料封包透過重播裝置選定特定 RRC 信令封包進行重播。而被重播的 RRC 信令它在 PDCP 層以上的訊息要和原始封包一樣。</p> <p>(9) 將 gNB 端設定 NEA2、NIA2 機密和完整性安全演算法為最優先選擇重複(2)~(8)測試。</p>	<p>(e) 測試步驟：</p> <p>(1) 在用戶設備設定支援 NIA1 和 NIA2 完整性安全演算法</p> <p>(2) 在 gNB 端設定 NIA1 完整性安全演算法為最優先選擇。</p> <p>(4) 確認 gNB 與 5GC 間建立 NGAP 連線，且用戶設備註冊 5G 網路。</p> <p>(6) 從擷取的 NG-RAN 介面資料封包透過重播裝置選定特定 RRC 信令封包(如 AS Security Mode Complete)進行重播。而被重播的 RRC 信令的 PDCP 內容(含 PDCP 計數與訊息完整性鑑別碼)要和原始封包一樣。</p> <p>(9) 將 gNB 端設定 NIA2 完整性安全演算法為最優先選擇重複(2)~(8)測試。</p>

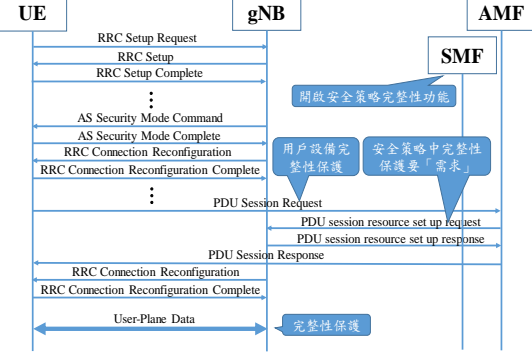
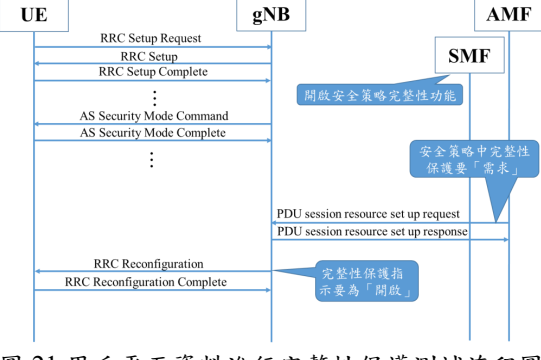
<p>6.1.1.4</p>	<p>(a) 透過重播裝置進行測試</p> <p>(b) 透過具備重播功能的用戶設備進行測試</p> <p>圖 9 RRC 信令重播攻擊保護測試流程圖</p>	<p>(a) 透過重播裝置進行測試</p> <p>(b) 透過具備重播功能的用戶設備進行測試</p> <p>圖 9 RRC 信令重播攻擊保護測試流程圖</p>
<p>6.1.2.1</p>	<p>(c) 測試前提：</p> <ol style="list-style-type: none"> (1) 用戶設備及 gNB 可進行完整性安全演算法設定。 (2) 用戶設備、gNB 及核心網路端可成功建立 5G 連線。 (3) 5GC 端的 SMF 要開啟用戶平面安全策略。 	<p>(c) 測試前提：</p> <ol style="list-style-type: none"> (1) 用戶設備及 gNB 間可以進行完整性安全演算法設定。 (2) 用戶設備、gNB 及 5GC 間可以成功建立 5G 連線。 (3) SMF 要開啟用戶平面安全策略之用戶平面完整性保護指示。
<p>6.1.2.1</p>	<p>(e) 測試步驟：</p> <ol style="list-style-type: none"> (4) gNB 與 5GC 建立 NGAP 連線，並確認用戶設備註冊上核心網路和傳送數據資料。 (7) 透過 NG-RAN 介面封包，確認用戶設備和 gNB 透過 RRC Connection Reconfiguration 完成用戶平面安全驗證程序。 (8) 透過 NG-RAN 介面封包，確認用戶設備和 gNB 間的用戶平面封包所對應的 PDCP 層的訊息帶有完整性鑑別碼。 	<p>(e) 測試步驟：</p> <ol style="list-style-type: none"> (4) 確認 gNB 與 5GC 間建立 NGAP 連線，且用戶設備註冊上 5GC 和傳送數據資料。 (7) 透過 NG-RAN 介面封包，確認用戶設備和 gNB 透過 RRC Reconfiguration 完成用戶平面安全驗證程序。 (8) 透過 NG-RAN 介面封包，確認用戶設備和 gNB 間的用戶平面封包所對應之 PDCP 層的訊息帶有完整性鑑別碼。
<p>6.1.2.1</p>	<p>圖 11 用戶數據資料完整性保護測試流程圖</p>	<p>圖 11 用戶數據資料完整性保護測試流程圖</p>

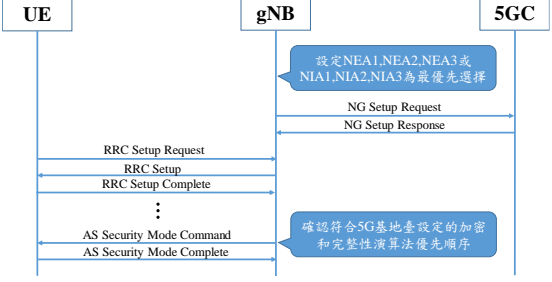
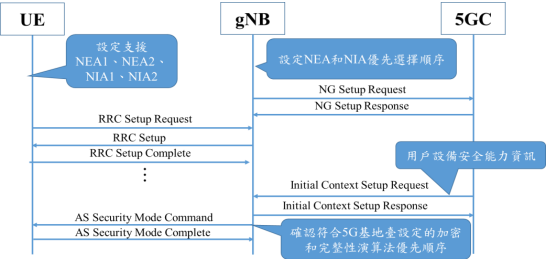
6.1.2.1	(f) 測試結果： (1) 根據步驟(7)，gNB 傳送的 RRC Connection Reconfiguration 中的完整性保護指示要為「開啟」，並且用戶設備回應 RRC Connection Reconfiguration Complete。	(f) 測試結果： (1) 根據步驟(7)，gNB 傳送的 RRC Reconfiguration 中的完整性保護指示要為「開啟」，並且用戶設備回應 RRC Reconfiguration Complete。
6.1.2.2	(c) 測試前提： (1) 用戶設備及 gNB 可進行完整性安全演算法設定。 (2) 用戶設備、gNB 及核心網路端可成功建立 5G 連線。 (3) 5GC 端的 SMF 要開啟用戶平面安全策略。	(c) 測試前提： (1) 用戶設備及 gNB 間可以進行完整性安全演算法設定。 (2) 用戶設備、gNB 及 5GC 間可以成功建立 5G 連線。 (3) SMF 要開啟用戶平面安全策略之用戶平面完整性保護指示。
6.1.2.2	(e) 測試步驟： (4) gNB 與 5GC 建立 NGAP 連線，並確認用戶設備註冊和傳送數據封包。 (5) 停止擷取 NG-RAN 介面封包。	(e) 測試步驟： (4) 確認 gNB 與 5GC 間建立 NGAP 連線，並確認且用戶設備註冊和傳送數據封包。 (5) 停止擷取 NG-RAN 介面封包。
6.1.2.2	 <p>圖 13 用戶平面完整性檢查失敗測試流程圖</p>	 <p>圖 13 用戶平面完整性檢查失敗測試流程圖</p>
6.1.2.3	(c) 測試前提： (1) 用戶設備及 gNB 可進行機密和完整性安全演算法設定。 (2) 用戶設備、gNB 及核心網路端可成功建立 5G 連線。 (3) 5GC 端的 SMF 如果要開啟用戶平面安全策略。	(c) 測試前提： (1) 用戶設備及 gNB 間可以進行機密和完整性安全演算法設定。 (2) 用戶設備、gNB 及核心網路端 5GC 間可以成功建立 5G 連線。 (3) 5GC 端的 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」。
6.1.2.3	(e) 測試步驟： (4) gNB 與 5GC 建立 NGAP 連線，並確認用戶設備註冊和傳送數據封包。 (7) 透過 NG-RAN 介面封包，確認用戶設備和 gNB 透過 RRC Connection Reconfiguration 完成用戶平面安全驗證程序。	(e) 測試步驟： (4) 確認 gNB 與 5GC 間建立 NGAP 連線，且用戶設備註冊和傳送數據封包。 (7) 透過 NG-RAN 介面封包，確認用戶設備和 gNB 透過 RRC Reconfiguration 完成用戶平面安全驗證程序。

<p>6.1.2.3</p>	 <p>圖 15 用戶平面資料加密測試流程圖</p>	 <p>圖 15 用戶平面資料加密測試流程圖</p>
<p>6.1.2.3</p>	<p>(f) 測試結果： (1) 根據步驟(7)，gNB 傳送的 RRC Connection Reconfiguration 中的關閉加密保護指示要為「關閉開啟」或不包含該指示，並且用戶設備回應 RRC Connection Reconfiguration Complete。</p>	<p>(f) 測試結果： (1) 根據步驟(7)，gNB 傳送的 RRC Reconfiguration 中的關閉加密保護指示要為「關閉」或不包含該指示，並且用戶設備回應 RRC Reconfiguration Complete。</p>
<p>6.1.2.4</p>	<p>(c) 測試前提： (1) 用戶設備及 gNB 可進行機密和完整性安全演算法設定。 (2) 用戶設備、gNB 及核心網路端可成功建立 5G 連線。 (3) 5GC 端的 SMF 要開啟用戶平面安全策略。</p>	<p>(c) 測試前提： (1) 用戶設備及 gNB 間可以進行機密和完整性安全演算法設定。 (2) 用戶設備、gNB 及 5GC 間可以成功建立 5G 連線。 (3) SMF 要開啟用戶平面安全策略之用戶平面完整性保護指示。</p>
<p>6.1.2.4</p>	 <p>圖 16 用戶數據資料重播攻擊保護測試示意圖</p>	 <p>(a) 透過重播裝置進行測試</p>  <p>(b) 透過具備重播功能的用戶設備進行測試</p> <p>圖 16 用戶數據資料重播攻擊保護測試示意圖</p>

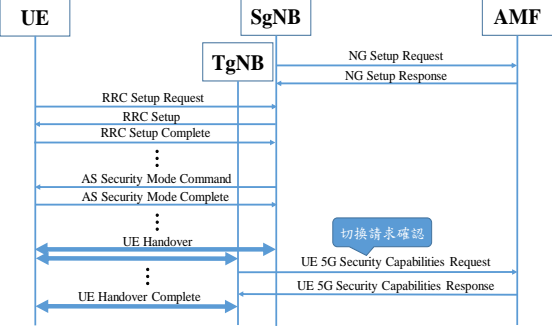
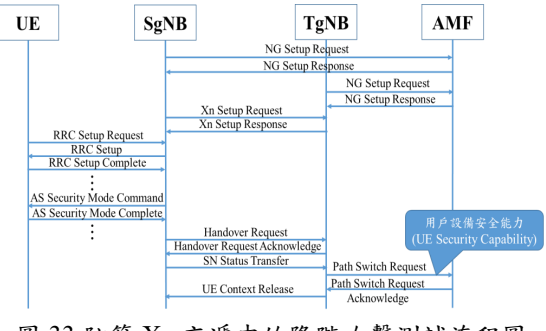
<p>6.1.2.4</p>	<p>(c) 測試步驟：</p> <p>(1) 在用戶設備設定支援 NEA1、NEA2、NIA1、NIA2 機密和完整性安全演算法。</p> <p>(2) 在 gNB 端設定 NEA1、NIA1 機密和完整性安全演算法為最優先選擇。</p> <p>(4) gNB 與 5GC 建立 NGAP 連線，並確認用戶設備註冊和傳送數據封包。</p> <p>(8) 將 gNB 端設定 NEA2、NIA2 機密和完整性安全演算法為最優先選擇重複(2)~(7)測試。</p>	<p>(c) 測試步驟：</p> <p>(1) 在用戶設備設定支援 NIA1、NIA2 完整性安全演算法。</p> <p>(2) 在 gNB 端設定 NIA1 完整性安全演算法為最優先選擇。</p> <p>(4) 確認 gNB 與 5GC 間建立 NGAP 連線，且用戶設備註冊和傳送數據封包。</p> <p>(8) 將 gNB 端設定 NIA2 完整性安全演算法為最優先選擇重複(2)~(7)測試。</p>
<p>6.1.2.4</p>	 <p>圖 17 用戶數據資料重播攻擊保護測試流程圖</p>	 <p>(a) 透過重播裝置進行測試</p>  <p>(b) 透過具備重播功能的用戶設備進行測試</p> <p>圖 17 用戶數據資料重播攻擊保護測試流程圖</p>
<p>6.1.2.5</p>	<p>(c) 測試前提：</p> <p>(1) 用戶設備及 gNB 可進行機密和完整性安全演算法設定。</p> <p>(2) 用戶設備、gNB 及核心網路端可成功建立 5G 連線。</p> <p>(3) 5GC 端的 SMF 要開啟用戶平面安全策略。</p> <p>(5) 測試人員可擷取 NGAP 封包並分析該封包內容。</p>	<p>(c) 測試前提：</p> <p>(1) 用戶設備及 gNB 間可以進行機密和完整性安全演算法設定。</p> <p>(2) 用戶設備、gNB 及 5GC 間可以成功建立 5G 連線。</p> <p>(3) SMF 要開啟用戶平面安全策略之用戶平面加密保護指示。</p> <p>(5) 測試人員可擷取 N2 介面封包並分析該封包內容。</p>

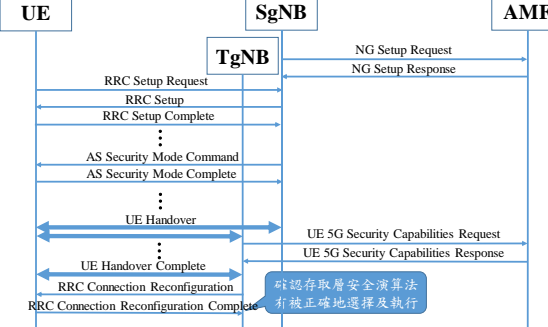
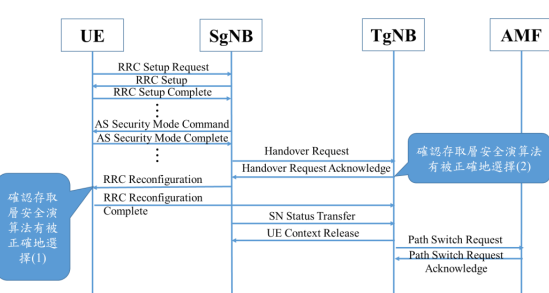
<p>6.1.2.5</p>	<p>(e) 測試步驟：</p> <p>(3) 開始擷取 NG-RAN 介面封包和 NGAP 封包。</p> <p>(4) gNB 與 5GC 建立下一代應用協定連線，並確認用戶設備註冊和傳送數據封包。</p> <p>(5) 停止擷取 NG-RAN 介面封包和 NGAP 封包。</p> <p>(7) 透過應用協定封包，確認 5GC 傳送給 gNB PDU Session Resource Set Up Request 帶有完整性保護需求的安全資訊。</p> <p>(8) 透過 NG-RAN 介面封包，確認 gNB 傳送給用戶設備 RRC Connection Reconfiguration 完整性保護指示是否符合程序(7) 加密保護需求。</p>	<p>(e) 測試步驟：</p> <p>(3) 開始擷取 NG-RAN 介面封包和 N2 介面封包。</p> <p>(4) 確認 gNB 與 5GC 建立 NGAP 連線，且用戶設備註冊和傳送數據封包。</p> <p>(5) 停止擷取 NG-RAN 介面封包和 N2 介面封包。</p> <p>(7) 透過 N2 介面封包，確認 5GC 傳送給 gNB PDU Session Resource Set Up Request 帶有完整性保護需求的安全資訊。</p> <p>(8) 透過 NG-RAN 介面封包，確認 gNB 傳送給用戶設備 RRC Reconfiguration 完整性保護指示是否符合程序(7) 加密保護需求。</p>
<p>6.1.2.5</p>	 <p>圖 19 用戶平面資料進行加密測試流程圖</p>	 <p>圖 19 用戶平面資料進行加密測試流程圖</p>
<p>6.1.2.5</p>	<p>(f) 測試結果：</p> <p>(1) 根據步驟(7)，AS Security Mode Command 裡面的安全演算法要符合 gNB 的安全演算法優先順序設定。</p>	<p>(f) 測試結果：</p> <p>(1) 根據步驟(7)，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」。</p> <p>(2) 根據步驟(8)，RRC Reconfiguration 關閉加密保護指示要符合程序 (7) 加密保護需求為「關閉」或不包含該指示。</p>
<p>6.1.2.6</p>	<p>(c) 測試前提：</p> <p>(1) 用戶設備及 gNB 可進行完整性安全演算法設定。</p> <p>(2) 用戶設備、gNB 及核心網路端可成功建立 5G 連線。</p> <p>(3) 5GC 端的 SMF 要開啓用戶平面安全策略。</p> <p>(5) 測試人員可擷取 NGAP 並分析該封包內容。</p>	<p>(c) 測試前提：</p> <p>(1) 用戶設備及 gNB 間可以進行完整性安全演算法設定。</p> <p>(2) 用戶設備、gNB 及 5GC 間可以成功建立 5G 連線。</p> <p>(3) SMF 要開啓用戶平面安全策略之用戶平面完整性保護指示。</p> <p>(5) 測試人員可擷取 N2 介面並分析該封包內容。</p>

<p>6.1.2.6</p>	<p>(e) 測試步驟：</p> <p>(3) 開始擷取 NG-RAN 介面封包和 NGAP 封包。</p> <p>(4) gNB 與 5GC 建立下一代應用協定連線，並確認用戶設備註冊和傳送數據封包。</p> <p>(5) 停止擷取 NG-RAN 介面封包和 NGAP 封包。</p> <p>(7) 透過應用協定封包，確認 5GC 傳送給 gNB PDU Session Resource Set Up Request 帶有完整性保護需求的安全資訊。</p> <p>(8) 透過 NG-RAN 介面封包，確認 gNB 傳送給用戶設備 RRC Connection Reconfiguration n 完整性保護指示是否符合程序(7) 加密保護需求。</p>	<p>(e) 測試步驟：</p> <p>(3) 開始擷取 NG-RAN 介面封包和 N2 介面封包。</p> <p>(4) 確認 gNB 與 5GC 建立 NGAP 連線，且用戶設備註冊和傳送數據封包。</p> <p>(5) 停止擷取 NG-RAN 介面封包和 N2 介面封包。</p> <p>(7) 透過 N2 介面封包，確認 5GC 傳送給 gNB PDU Session Resource Set Up Request 帶有完整性保護需求的安全資訊。</p> <p>(8) 透過 NG-RAN 介面封包，確認 gNB 傳送給用戶設備 RRC Reconfiguration 完整性保護指示是否符合程序(7) 加密保護需求。</p>
<p>6.1.2.6</p>	 <p>圖 21 用戶平面資料進行完整性保護測試流程圖</p>	 <p>圖 21 用戶平面資料進行完整性保護測試流程圖</p>
<p>6.1.2.6</p>	<p>(f) 測試結果：</p> <p>(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」。</p>	<p>(f) 測試結果：</p> <p>(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「需求」。</p> <p>(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」。</p>
<p>6.1.3.1</p>	<p>(c) 測試前提：</p> <p>(1) 用戶設備及 gNB 可進行機密和完整性安全演算法設定。</p> <p>(2) 用戶設備、gNB 及核心網路端可成功建立 5G 連線。</p> <p>(4) 測試人員可擷取 NGAP 封包並分析該封包內容。</p>	<p>(c) 測試前提：</p> <p>(1) 用戶設備及 gNB 間可以進行機密和完整性安全演算法設定。</p> <p>(2) 用戶設備、gNB 及 5GC 間可以成功建立 5G 連線。</p> <p>(4) 測試人員可擷取 N2 介面封包並分析該封包內容。</p>

<p>6.1.3.1</p>	<p>(e) 測試步驟：</p> <p>(3) 開始擷取 NG-RAN 介面封包和 NGAP 封包。</p> <p>(4) gNB 與 5GC 建立 NGAP 連線，並確認用戶設備註冊上核心網路。</p> <p>(5) 停止擷取 NG-RAN 介面封包和 NGAP 封包。</p> <p>(6) 透過應用協定封包，確認 5GC 傳送給 gNB 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。</p>	<p>(e) 測試步驟：</p> <p>(3) 開始擷取 NG-RAN 介面封包和 N2 介面封包。</p> <p>(4) 確認 gNB 與 5GC 建立 NGAP 連線，且用戶設備註冊上 5GC。</p> <p>(5) 停止擷取 NG-RAN 介面封包和 N2 介面封包。</p> <p>(6) 透過 N2 介面封包，確認 5GC 傳送給 gNB 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。</p>
<p>6.1.3.1</p>	 <p>圖 23 加密和完整性演算法優先順序測試流程圖</p>	 <p>圖 23 加密和完整性演算法優先順序測試流程圖</p>
<p>6.1.3.2</p>	<p>6.1.3.2 gNB 金鑰更新-封包資料匯聚通訊協定 (PDCP)計數環繞</p> <p>(a) 測試依據：</p> <p>依據 3GPP TS 33.501 [6] 之第 6.9.4.1 小節與 TS 38.331 [8] 之第 5.3.1.2 小節以及 3GPP TR 33.926 [7] 之第 D.2.2.7 小節，並參考 3GPP TS 33.511 [1] 之第 4.2.2.1.13 小節。</p> <p>.....</p>	<p>6.1.3.2 gNB 金鑰更新-封包資料匯聚通訊協定 (PDCP)計數環繞</p> <p>3GPP TS 33.501 [6] 已經刪除第 6.9.4.1 小節之資安測試需求</p>
<p>6.1.3.3</p>	<p>(c) 測試前提：</p> <p>(1) 用戶設備及 gNB 可進行完整性安全演算法設定。</p> <p>(2) 用戶設備、gNB 及核心網路端可成功建立 5G 連線。</p> <p>(3) 5GC 端的 SMF 要開啟用戶平面安全策略。</p> <p>(5) 測試人員可擷取 NGAP 封包並分析該封包內容。</p>	<p>(c) 測試前提：</p> <p>(1) 用戶設備及 gNB 間可以進行完整性安全演算法設定。</p> <p>(2) 用戶設備、gNB 及 5GC 間可以成功建立 5G 連線。</p> <p>(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」。</p> <p>(5) 測試人員可擷取 N2 介面封包並分析該封包內容。</p>

<p>6.1.3.3</p>	<p>(e) 測試步驟：</p> <p>(3) 開始擷取 NG-RAN 介面封包和 NGAP 封包。</p> <p>(4) gNB 與 5GC 建立 NGAP 連線，並確認用戶設備註冊上核心網路和傳送數據資料。</p> <p>(6) 停止擷取 NG-RAN 介面封包和 NGAP 封包。</p> <p>(7) 透過 NG-RAN 介面和 NGAP 封包，確認 gNB 啟動蜂巢間 (intra cell) 換手程序進行 KRRC-enc, KRRC-int, KUP-enc, and KUP-int 更新。</p>	<p>(e) 測試步驟：</p> <p>(3) 開始擷取 NG-RAN 介面封包。</p> <p>(4) 確認與 5GC 間建立 NGAP 連線，且用戶設備註冊上 5GC 和傳送數據資料。</p> <p>(6) 停止擷取 NG-RAN 介面封包。</p> <p>(7) 透過 NG-RAN 介面封包，確認 gNB 發生 PDCP 重建進行 K_{gNB} 更新。</p>
<p>6.1.3.3</p>	<p>圖 27 gNB 金鑰更新測試流程圖</p>	<p>圖 27 gNB 金鑰更新測試流程圖</p>
<p>6.1.3.3</p>	<p>(f) 測試結果：</p> <p>(1) 根據步驟(7)，當無線電承載識別碼重覆使用後，在無線接取介面看到 KRRC-enc, KRRC-int, KUP-enc, and KUP-int 值發生更新代表 K_{gNB} 發生更新避免訊息洩露。</p>	<p>(f) 測試結果：</p> <p>(1) 根據步驟(7)，當無線電承載識別碼重覆使用後，在無線接取介面看到 PDCP 重建因此 gNB 進行 K_{gNB} 更新避免訊息洩露。</p>
<p>6.1.3.4</p>	<p>(c) 測試前提：</p> <p>(2) 用戶設備及 gNB 可進行完整性安全演算法設定。</p> <p>(3) 用戶設備、gNB 及核心網路端可成功建立 5G 連線。</p> <p>(4) 5GC 端的 SMF 要開啓用戶平面安全策略。</p>	<p>(c) 測試前提：</p> <p>(2) 用戶設備及 gNB 間可以進行完整性安全演算法設定。</p> <p>(3) 用戶設備、gNB 及 5GC 間可以成功建立 5G 連線。</p> <p>(4) SMF 如果要開啓用戶平面安全策略，其用戶平面資料加密保護指示不能設定為「停用」。</p>
<p>6.1.3.4</p>	<p>(e) 測試步驟：</p> <p>(4) gNB 與 5GC 建立下一代應用協定連線，並進行用戶設備註冊。</p> <p>(8) 透過 NG-RAN 介面和 XnAP，觀察 Xn 應用協定是否啟動次節點金鑰更新流程及 KSN 值狀態。</p>	<p>(e) 測試步驟：</p> <p>(4) 確認 gNB 與 5GC 建立 NGAP 連線，且用戶設備註冊上 5GC 和傳送數據資料。</p> <p>(8) 透過 NG-RAN 介面和 Xn 介面，觀察 Xn 應用協定是否啟動次節點金鑰更新流程及 KSN 值狀態。</p>

6.1.3.5	(c) 測試前提： (3) 用戶設備、gNB 及核心網路端可成功建立 5G 連線。 (4) 5GC 端的 SMF 要開啟用戶平面安全策略。	(c) 測試前提： (3) 用戶設備、gNB 及核心網路 5GC 端可成功建立 5G 連線。 (4) 5GC 端的 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」。
6.1.3.5	(e) 測試步驟： (4) gNB 與 5GC 建立 NGAP 連線，並進行用戶設備註冊。	(e) 測試步驟： (4) 確認 gNB 與 5GC 間建立 NGAP 連線，並進行且用戶設備註冊上 5GC 和傳送數據資料。
6.1.4.1	(c) 測試前提： (2) gNB 可支援 Xn 介面換手。 (3) 用戶設備、gNB 及核心網路端可成功建立 5G 連線。 (4) 測試人員可擷取 NG-RAN 介面封包，並分析 RRC 封包之 PCDP 層的內容。 (5) 測試人員可擷取 NGAP 封包並分析其內容。 (6) 測試人員可擷取 XnAP 封包並分析其內容。	(c) 測試前提： (2) gNB 可以支援 Xn 介面換手 (3) 用戶設備、gNB 及 5GC 間可以成功建立 5G 連線。 (4) 測試人員可擷取 N2 介面封包並分析其內容。 (5) 測試人員可擷取 Xn 介面封包並分析其內容。
6.1.4.1	(e) 測試步驟： (3) 開始擷取 NG-RAN 介面、NGAP 和 XnAP 的封包。 (4) 來源 gNB 及目的 gNB 與 5GC 建立 NGAP 連線，並用戶設備與來源 gNB 進行註冊。 (6) 停止擷取 NG-RAN 介面、NGAP 和 XnAP 的封包。 (7) 透過 XnAP 的封包，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。	(e) 測試步驟： (3) 開始擷取 N2 介面和 Xn 介面的封包。 (4) 確認來源 gNB 及目的 gNB 分別與 5GC 建立 NGAP 連線，來源 gNB 及目的 gNB 間建立 XnAP 連線，且用戶設備透過來源 gNB 註冊上 5GC。 (6) 停止擷取 N2 介面和 Xn 介面的封包。 (7) 透過 N2 介面的封包，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。
6.1.4.1	 <p>圖 33 防範 Xn 交遞中的降階攻擊測試流程圖</p>	 <p>圖 33 防範 Xn 交遞中的降階攻擊測試流程圖</p>

<p>6.1.4.2</p>	<p>(c) 測試前提：</p> <p>(1) 用戶設備、來源 gNB 及目的 gNB 可進行存取層安全演算法設定。</p> <p>(2) gNB 可支援 Xn 介面換手。</p> <p>(3) 用戶設備、gNB 及核心網路端 5GC 可以成功建立 5G 連線。</p> <p>(5) 測試人員可擷取 NGAP 封包並分析其內容。</p> <p>(6) 測試人員可擷取 XnAP 封包並分析其內容。</p>	<p>(c) 測試前提：</p> <p>(1) 用戶設備、來源 gNB 及目的 gNB 間可以進行存取層安全演算法設定。</p> <p>(2) gNB 可以支援 Xn 介面換手。</p> <p>(3) 用戶設備、gNB 及 5GC 可以成功建立 5G 連線。</p> <p>(5) 測試人員可擷取 N2 介面封包並分析其內容。</p> <p>(6) 測試人員可擷取 Xn 介面封包並分析其內容。</p>
<p>6.1.4.2</p>	<p>(e) 測試步驟：</p> <p>(3) 開始擷取 NG-RAN 介面、NGAP 和 XnAP 的封包。</p> <p>(4) 來源 gNB 及目的 gNB 與 5GC 建立 NG-RAN 連線，並用戶設備與來源 gNB 進行註冊。</p> <p>(6) 停止擷取 NG-RAN 介面、NGAP 和 XnAP 的封包。</p> <p>(7) 透過 NG-RAN 介面，檢查 RRC Connection Reconfiguration 中的目的 gNB 的加密和完整性安全演算法。並且確認用戶設備回復 RRC Connection Reconfiguration Complete。</p>	<p>(e) 測試步驟：</p> <p>(3) 開始擷取 NG-RAN 介面、N2 介面和 Xn 介面的封包。</p> <p>(4) 確認來源 gNB 及目的 gNB 與 5GC 建立 NG-RAN 連線，且用戶設備透過來源 gNB 註冊上 5GC。</p> <p>(6) 停止擷取 NG-RAN 介面、N2 介面和 Xn 介面的封包。</p> <p>(7) 透過 NG-RAN 介面或 Xn 介面，檢查 RRC Reconfiguration 或 Handover Request Acknowledge(Handover Command)中的目的 gNB 的加密和完整性安全演算法。</p>
<p>6.1.4.2</p>	 <p>圖 33 在 Xn 交遞中存取層安全演算法選擇測試流程圖</p>	 <p>圖 33 在 Xn 交遞中存取層安全演算法選擇測試流程圖</p>
<p>6.1.4.2</p>	<p>(f) 測試結果：</p> <p>(1) 根據步驟(7)，RRC Connection Reconfiguration 中的目的 gNB 的加密和完整性安全演算法要符合目的 gNB 的安全演算法優先順序設定。</p> <p>(2) 並且用戶設備會回復 RRC Connection Reconfiguration Complete。</p>	<p>(f) 測試結果：</p> <p>(1) 根據步驟(7)，RRC Reconfiguration 或 Handover Request Acknowledge(Handover Command)中的目的 gNB 的加密和完整性安全演算法要符合目的 gNB 的安全演算法優先順序設定。</p>



6.1.5.1	<p>(c) 測試前提：</p> <p>(1) 用戶設備及 gNB 可進行存取層安全演算法設定。</p> <p>(2) 安全閘道器 (Security Gateway) 用戶端及伺服器端可支援 IKEv2，並可進行 IPsec 安全演算法設定。</p> <p>(3) 安全閘道器用戶端及伺服器端可成功建立 IPsec 連線。</p> <p>(4) 用戶設備、gNB 及核心網路端可透過 IPsec 成功建立 5G 連線。</p>	<p>(c) 測試前提：</p> <p>(1) 用戶設備及 gNB 間可以進行存取層安全演算法設定。</p> <p>(2) 安全閘道器 (Security Gateway) 用戶端及伺服器端都可以支援 IKEv2，並可進行 IPsec 安全演算法設定。</p> <p>(3) 安全閘道器用戶端及伺服器之間可以成功建立 IPsec 連線。</p> <p>(4) 用戶設備、gNB 及 5GC 間可以透過 IPsec 成功建立 5G 連線。</p>
6.1.5.1	<p>(f) 測試結果：</p> <p>(1) 根據步驟(7)，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，其演算法強弱分為最低必須支援的 Shall 和建議支援的 Should。</p> <p>(2) 根據步驟(7)，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 的第二階段加密演算法應符合以下標準。其中演算法強弱分為最低必須支援的 Shall 和建議支援的 Should，標記+代表演算法強度更強。</p> <p>iii AES-GCM with a 16 octet ICV with 128-bit key length - Should</p> <p>iv AES-GCM with a 16 octet ICV with 256-bit key length - Should+</p>	<p>(f) 測試結果：</p> <p>(1) 根據步驟(7)，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。</p> <p>(2) 根據步驟(7)，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 的第二階段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。</p> <p>iii AES-GCM with a 16 octet ICV with 128-bit key length - Shall</p> <p>iv AES-GCM with a 16 octet ICV with 256-bit key length - Shall+</p>
6.1.5.2	<p>(c) 測試前提：</p> <p>(1) 用戶設備及 gNB 可進行存取層安全演算法設定。</p> <p>(2) 安全閘道器 (Security Gateway) 的用戶端及伺服器可成功建立 IPsec 連線。</p> <p>(3) 安全閘道器的用戶端及伺服器可支援 IKEv2，並可進行 IPsec 安全演算法設定。</p> <p>(4) 用戶設備、gNB 及核心網路端可透過 IPsec 成功建立 5G 連線。</p>	<p>(c) 測試前提：</p> <p>(1) 用戶設備及 gNB 間可以進行存取層安全演算法設定。</p> <p>(2) 安全閘道器 (Security Gateway) 的用戶端及伺服器之間可以成功建立 IPsec 連線。</p> <p>(3) 安全閘道器的用戶端及伺服器都可以支援 IKEv2，並可進行 IPsec 安全演算法設定。</p> <p>(4) 用戶設備、gNB 及 5GC 間可以透過 IPsec 成功建立 5G 連線。</p>



<p>6.1.5.2</p>	<p>(f) 測試結果：</p> <p>(1) 根據步驟(7)，IKE-SA-INIT 請求信令中含有 IKEv2 的第一階段加密演算法需要符合以下標準。根據 3GPP REL 15 與 REL 16，其演算法強弱分為最低必須支援的 Shall 和建議支援的 Should。</p> <p>(2) 根據步驟(7)，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 的第二階段加密演算法需要符合以下標準。其中演算法強弱分為最低必須支援的 Shall 和建議支援的 Should，標記+代表演算法強度更強。</p> <p>iii AES-GCM with a 16 octet ICV with 128-bit key length - Should</p> <p>iv AES-GCM with a 16 octet ICV with 256-bit key length - Should+</p>	<p>(f) 測試結果：</p> <p>(1) 根據步驟(7)，IKE-SA-INIT 請求信令中含有 IKEv2 的第一階段加密演算法需要符合以下標準。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。</p> <p>(2) 根據步驟(7)，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 的第二階段加密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，標記+代表演算法強度更強。</p> <p>iii AES-GCM with a 16 octet ICV with 128-bit key length - Shall</p> <p>iv AES-GCM with a 16 octet ICV with 256-bit key length - Shall+</p>
<p>6.1.5.3</p>	<p>(c) 測試前提：</p> <p>(1) 用戶設備、來源 gNB 及目的 gNB 可進行存取層安全演算法設定。</p> <p>(2) 安全閘道器 (Security Gateway) 的用戶端及伺服器可成功建立 IPsec 連線。</p> <p>(3) Xn 介面相關的安全閘道器的用戶端及用戶端可成功建立 IPsec 連線。</p> <p>(4) Xn 介面相關的安全閘道器的用戶端及伺服器可支援 IKEv2 並可進行 IPsec 安全演算法設定。</p> <p>(5) Xn 介面相關的安全閘道器的用戶端及用戶端可支援 IKEv2 並可進行 IPsec 安全演算法設定。</p> <p>(7) 用戶設備、gNB 及核心網路端可透過 IPsec 成功建立 5G 連線。</p>	<p>(c) 測試前提：</p> <p>(1) 用戶設備、來源 gNB 及目的 gNB 間可以進行存取層安全演算法設定。</p> <p>(2) 安全閘道器 (Security Gateway) 的用戶端及伺服器之間可以成功建立 IPsec 連線。</p> <p>(3) Xn 介面相關的安全閘道器的用戶端及用戶端之間可以成功建立 IPsec 連線。</p> <p>(4) Xn 介面相關的安全閘道器的用戶端及伺服器都可以支援 IKEv2 並可進行 IPsec 安全演算法設定。</p> <p>(5) Xn 介面相關的安全閘道器的用戶端及用戶端都可以支援 IKEv2 並可進行 IPsec 安全演算法設定。</p> <p>(7) 用戶設備、gNB 及 5GC 端可透過 IPsec 成功建立 5G 連線。</p>

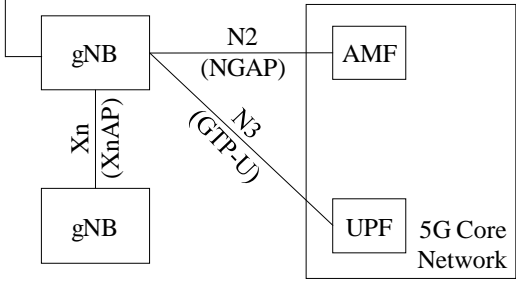
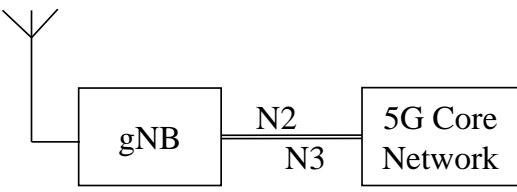


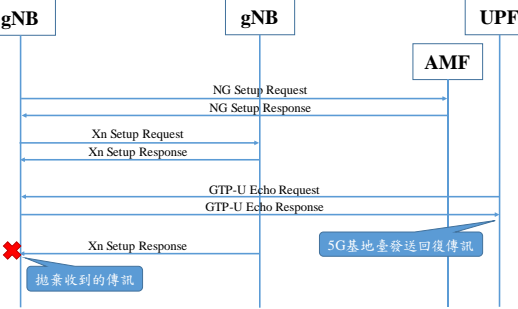
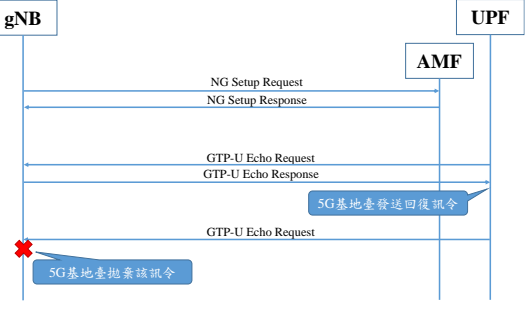
<p>6.1.5.3</p>	<p>(f) 測試結果：</p> <p>(1) 透過步驟(7)，IKE-SA-INIT 請求信令中含有 IKEv2 的第一階段加密演算法需要符合以下標準。根據 3GPP REL 15 與 REL 16，其演算法強弱分為最低必須支援的 Shall 和建議支援的 Should。</p> <p>(2) 透過步驟(7)，IKE-AUTH 是由 IKEv2 的第一階段加密演算法進行機密性保護。解密後的 IKE-AUTH 請求信令中含有 IKEv2 的第二階段加密演算法需要符合以下標準。其中演算法強弱分為最低必須支援的 Shall 和建議支援的 Should，標記+代表演算法強度更強。</p> <p>iii AES-GCM with a 16 octet ICV with 128-bit key length – Should</p> <p>iv AES-GCM with a 16 octet ICV with 256-bit key length - Should+</p>	<p>(f) 測試結果：</p> <p>(1) 透過步驟(7)，IKE-SA-INIT 請求信令中含有 IKEv2 的第一階段加密演算法需要符合以下標準。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。</p> <p>(2) 透過步驟(7)，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 的第二階段加密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，標記+代表演算法強度更強。</p> <p>iii AES-GCM with a 16 octet ICV with 128-bit key length – Shall</p> <p>iv AES-GCM with a 16 octet ICV with 256-bit key length - Shall+</p>
<p>6.1.5.4</p>	<p>(c) 測試前提：</p> <p>(1) 用戶設備及 gNB 可進行存取層安全演算法設定。</p> <p>(2) 安全閘道器 (Security Gateway) 的用戶端及伺服器端可支援 IKEv2，並可進行際網路安全協定安全演算法設定。</p> <p>(3) 安全閘道器用戶端及伺服器端可成功建立 IPsec 連線。</p> <p>(4) 用戶設備、gNB 及核心網路端可透過 IPsec 成功建立 5G 連線。</p>	<p>(c) 測試前提：</p> <p>(1) 用戶設備及 gNB 間可以進行存取層安全演算法設定。</p> <p>(2) 安全閘道器 (Security Gateway) 的用戶端及伺服器端之間可以支援 IKEv2，並可進行際網路安全協定安全演算法設定。</p> <p>(3) 安全閘道器用戶端及伺服器端之間可以成功建立 IPsec 連線。</p> <p>(4) 用戶設備、gNB 及核心網路 5GC 端間可以透過 IPsec 成功建立 5G 連線。</p>




<p>6.1.5.4</p>	<p>(f) 測試結果：</p> <p>(1) 透過步驟(7)，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，其中演算法強弱分為最低必須支援的 Shall 和建議支援的 Should。</p> <p>(2) 透過步驟(7)，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。其中演算法強弱分為最低必須支援的 Shall 和建議支援的 Should，標記+代表演算法強度更強。</p> <p>i AUTH_HMAC_SHA1_96 - Shall ii AUTH_HMAC_SHA2_256_128 - Should iii AUTH_HMAC_SHA2_512_256 - Should+</p>	<p>(f) 測試結果：</p> <p>(1) 透過步驟(7)，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。</p> <p>(2) 透過步驟(7)，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。</p> <p>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</p>
<p>6.1.5.5</p>	<p>(c) 測試前提：</p> <p>(1) 用戶設備及 gNB 可進行存取層安全演算法設定。</p> <p>(2) 安全閘道器 (Security Gateway) 的用戶端及伺服器端可成功建立 IPsec 連線。</p> <p>(3) 安全閘道器的用戶端及伺服器端可支援 IKEv2，並可進行 IPsec 安全演算法設定。</p> <p>(4) 用戶設備、gNB 及核心網路端可透過 IPsec 成功建立 5G 連線。</p>	<p>(c) 測試前提：</p> <p>(1) 用戶設備及 gNB 間可以進行存取層安全演算法設定。</p> <p>(2) 安全閘道器 (Security Gateway) 的用戶端及伺服器之間可以成功建立 IPsec 連線。</p> <p>(3) 安全閘道器的用戶端及伺服器端都可以支援 IKEv2，並可進行 IPsec 安全演算法設定。</p> <p>(4) 用戶設備、gNB 及 5GC 間可以透過 IPsec 成功建立 5G 連線。</p>

<p>6.1.5.5</p>	<p>(f) 測試結果：</p> <p>(1) 根據步驟(7)，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，其中演算法強弱分為最低必須支援的 Shall 和建議支援的 Should。</p> <p>(2) 根據步驟(7)，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。其中演算法強弱分為最低必須支援的 Shall 和建議支援的 Should，標記為+代表演算法強度更強。</p> <p>i AUTH_HMAC_SHA1_96 - Shall ii AUTH_HMAC_SHA2_256_128 - Should iii AUTH_HMAC_SHA2_512_256 - Should+</p>	<p>(f) 測試結果：</p> <p>(1) 根據步驟(7)，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。</p> <p>(2) 根據步驟(7)，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，標記為+代表演算法強度更強。</p> <p>i AUTH_HMAC_SHA2_256_128 - 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 - Shall iv AUTH_HMAC_SHA2_512_256 - Should</p>
<p>6.1.5.6</p>	<p>(c) 測試前提：</p> <p>(1) 用戶設備及 gNB 可進行存取層安全演算法設定。</p> <p>(2) 安全閘道器 (Security Gateway) 用戶端及伺服器端可支援 IKEv2，並可進行 IPsec 安全演算法設定。</p> <p>(3) 安全閘道器用戶端及伺服器端可成功建立 IPsec 連線。</p> <p>(4) 用戶設備、gNB 及核心網路端可透過 IPsec 成功建立 5G 連線。</p>	<p>(c) 測試前提：</p> <p>(1) 用戶設備及 gNB 間可以進行存取層安全演算法設定。</p> <p>(2) 安全閘道器 (Security Gateway) 用戶端及伺服器端都可以支援 IKEv2，並可進行 IPsec 安全演算法設定。</p> <p>(3) 安全閘道器用戶端及伺服器之間可以成功建立 IPsec 連線。</p> <p>(4) 用戶設備、gNB 及 5GC 間可以透過 IPsec 成功建立 5G 連線。</p>

<p>6.1.5.6</p>	<p>(f) 測試結果：</p> <p>(1) 透過步驟(7)，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，其中演算法強弱分為最低必須支援的 Shall 和建議支援的 Should。</p> <p>(2) 透過步驟(7)，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。其中演算法強弱分為最低必須支援的 Shall 和建議支援的 Should。標記+代表演算法強度更強。</p> <p>i AUTH_HMAC_SHA1_96 - Shall ii AUTH_HMAC_SHA2_256_128 - Should iii AUTH_HMAC_SHA2_512_256 - Should+</p>	<p>(f) 測試結果：</p> <p>(1) 透過步驟(7)，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。</p> <p>(2) 透過步驟(7)，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。</p> <p>i AUTH_HMAC_SHA2_256_128 - 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 – Shall iv AUTH_HMAC_SHA2_512_256 - Should</p>
<p>6.1.6.1</p>	<p>(c) 測試前提：</p> <p>(1) gNB 具備兩個以上 GTP-U 資訊的網路傳輸介面。</p> <p>(3) 可以抓取 gNB 之 N3 介面與 Xn 介面的 GTP-U 封包。</p>	<p>(c) 測試前提：</p> <p>(1) gNB 具備一個以上 GTP-U 資訊的網路傳輸介面。</p> <p>(3) 可以抓取 gNB 之網路傳輸介面(如 N3 介面的)的 GTP-U 封包。</p>
<p>6.1.6.1</p>	 <p>圖 46 GTP-U 封包過濾功能測試示意圖</p>	 <p>圖 46 GTP-U 封包過濾功能測試示意圖</p>

<p>6.1.6.1</p>	<p>(e) 測試步驟：</p> <p>(1) 設定一個 N3 介面 (或 Xn 介面) 允許其能夠接收 GTP-U Echo Request 信令，同時設定其他 N3 介面或 Xn 介面禁止其能夠接收 GTP-U Echo Request 信令。</p> <p>(2) 對設定允許接收之 N3 介面或 Xn 介面傳送 GTP-U Echo Request 信令，成功收到來自 gNB 發送之 GTP-U Echo Response 信令。</p> <p>(3) 對設定禁止接收之 N3 介面或 Xn 介面傳送 GTP-U Echo Request 信令，gNB 拋棄該信令。</p>	<p>(e) 測試步驟：</p> <p>(1) 設定 gNB 的一個 N3 介面只允許其能夠接收 GTP-U Echo Request 信令。</p> <p>(2) UPF 對 gNB 設定允許接收之 N3 介面傳送 GTP-U Echo Request 信令，UPF 成功收到來自 gNB 發送之 GTP-U Echo Response 信令。</p> <p>(3) 設定 gNB 的一個 N3 介面禁止其能夠接收任何 GTP-U 信令。</p> <p>(4) UPF 對 gNB 設定禁止接收之 N3 介面傳送 GTP-U Echo Request 信令，gNB 拋棄該 GTP-U Echo Request 信令，故 UPF 將不會收到 GTP-U Echo Response。</p>
<p>6.1.6.1</p>	 <p>圖 49 GTP-U 封包過濾功能測試流程圖</p>	 <p>圖 49 GTP-U 封包過濾功能測試流程圖</p>
<p>6.1.6.1</p>	<p>(f) 測試結果：</p> <p>(1) 對於設定禁止接收之 N3 介面或 Xn 介面，gNB 拋棄收到的 GTP-U Echo Request 信令。</p> <p>(2) 對於設定允許接收之 N3 介面或 Xn 介面，gNB 發送 GTP-U Echo Response 信令。</p>	<p>(f) 測試結果：</p> <p>(1) 對於設定禁止接收之 N3 介面，gNB 拋棄收到的 GTP-U Echo Request 信令後，不會對 UPF 發送 GTP-U Echo Response。</p> <p>(2) 對於設定允許接收之 N3 介面，gNB 成功收到 GTP-U Echo Request 信令後，對 UPF 發送 GTP-U Echo Response 信令。</p>
<p>6.1.6.4</p>	<p>(c) 測試前提：</p> <p>(1) gNB 可成功與核心網路端建立 5G 連線。</p>	<p>(c) 測試前提：</p> <p>(1) gNB 可成功與 5GC 端建立 5G 連線。</p>



台灣資通產業標準協會

Taiwan Association of Information and Communication Standards

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