會議報告（出國類別：其他）

出席第三代合作夥伴計畫
3GPP SA3 #96 國際標準會議報告

出國單位：財團法人工業技術研究院

出席人員：陳瓊璋

派赴地區：華沙/弗次瓦夫

會議期間：108 年 8 月 26 日至 108 年 8 月 30 日

報告日期：108 年 9 月 27 日

摘 要

本團隊出席於2019年8月26日~8月30日在華沙/弗次瓦夫舉辦的第三代合作夥伴計畫(3rd Generation Partnership Project, 3GPP) 加密 (Security) 第三工作小組第96次會議(SA3 #96),本次會議由3GPP的歐洲友人(European Friends of 3GPP)舉辦，包含： Deutsche Telekom、Ericsson、Huawei、Intel、Nokia、Orange、Qualcomm等公司，此次會議約有200人與會，本團隊依規劃有1位成員出席會議。此行主要任務在於參與第五代行動通訊(5th Generation mobile communication, 5G)網路加密技術討論，關注5G在網路切片、網路功能虛擬化(Network Function Virtualization, NFV)、邊緣運算、衛星與無人機應用、火車/高鐵專屬通信應用等3GPP網路開放至各垂直領域應用加密技術標準制定狀況。由於5G讓越來越多裝置能夠與物聯網互通，並且共享資料和數據，使得許多人對於物聯網資料的安全防護堪憂；另外5G核心網路功能走向軟體化，使用了許多現有企業資訊技術(Information Technology, IT)關鍵技術，使得過去運用在IT時可能會出現的安全漏洞與威脅挑戰，未來也可能會在5G網路上出現，因此5G加密資安技術的確保顯得特別重要，對於5G應用的促進發展很有助益，值得本團隊持續追蹤。

縮寫與中英文對照表

英文全稱	英文縮寫	中文全稱
3rd Generation Partnership Project	3GPP	第三代合作夥伴計畫
5G New Radio Technology	5G NR	5G 新無線電技術
5th Generation mobile communication	5G	第五代行動通訊
Authentication Authorization Accounting	AAA	認證授權與計費
Access and Mobility Management Function	AMF	接入移動管理功能
Elliptic Curve- based Certificateless Signatures for Identity-based Encryption	ECCSI	橢圓曲線無證書簽名憑證
Extensible Authentication Protocol	EAP	擴展認證協議
Denial-of-Service	DoS	阻斷服務攻擊
Core Network	CN	核心網路
Internet Protocol Security	IPsec	網際網路安全協定
European Telecommunications Standards Institute	ETSI	歐洲電信標準協會
enhanced Mobile BroadBand	eMBB	增強型行動寬頻
Network Function Virtualization	NFV	網路功能虛擬化
Non-Access Stratum	NAS	非接入層
User Plane Function	UPF	用戶面功能
Virtual Private Network	VPN	虛擬私有網路
New Radio Technology	NR	新無線電技術
Security 3th Working Group	SA3	加密第三工作組
System Information	SI	系統信息
Performance Enhancing Proxies	PEP	效能增強代理器
Release 15	R15, Rel-15	第 15 版
Release 16	R16, Rel-16	第 16 版
Radio Access Network	RAN	無線存取網路
Study Item	SI	研究項目
Single Network Slice Selection Assistance Information	S-NSSAI	網路切片輔助選擇資訊
Technical Report	TR	技術報告
Work Item	WI	工作項目
Coordinated Universal Time	UTC	世界協調時間
Unified Data Management	UDM	統一數據管理

技術貢獻

此次是本團隊首次參加 SA3 會議，以掌握 3GPP 5G 加密資安技術標準制定狀況及發展方向、以及如何落地應用至垂直行業為主。

會議解說

- **SA3 工作小組完成 5G 第一階段增強型行動寬頻(Enhanced Mobile Broadband) eMBB 安全增強規格**

3GPP 完成了 5G 第一階段 eMBB 應用之網路傳輸技術規格，SA3 也據此完成 eMBB 應用安全增強規格(相對於 4G)，主要包括:

- 主要認證(Primary authentication)
- 次要認證(Secondary authentication)
- 運營商間加密(Inter-operator security)
- 以服務為基礎架構(Service based architecture)
- 資安密鑰階層(Key hierarchy)
- 移動性(Mobility)

主要技術規格文件為3GPP TS 33.501。

- **SA3 工作小組開始第二階段資安規格制訂**

由於 5G 讓越來越多裝置能夠與物聯網 互通，並且共享資料和數據，使得許多人對於物聯網資料的安全防護堪憂；另外 5G 核心網路功能走向軟體化，使用了許多現有企業資訊技術(Information Technology, IT)關鍵技術，使得過去運用在 IT 時可能會出現的安全漏洞與威脅挑戰，未來也可能會在 5G 網路上出現。因此目前 SA3 工作小組的資安規格制定主要方向包括:

- 物聯網
- 網路切片

- 網路功能虛擬化(Network Function Virtualization, NFV)
- 邊緣運算
- 衛星與無人機應用等低時延高可靠應用
- 火車/高鐵專屬通信等垂直領域應用

目　錄

摘 要.....1

縮寫與中英文對照表 2

技術貢獻.....3

會議解說.....3

一、會議名稱.....6

二、參加會議目的及效益 6

三、會議時間.....6

四、會議地點.....6

五、會議議程.....6

六、會議紀要.....9

七、心得與建議 9

一、會議名稱

3GPP SA3#96Meeting

二、參加會議目的及效益

參與在華沙/弗次瓦夫舉辦的 3GPP SA3#96 會議，本計畫團隊主要目的在於掌握 3GPP 5G 加密資安技術標準制定狀況及發展方向、以及如何落地應用至垂直行業為主。

三、會議時間

Aug 26, 2019 ~ Aug. 30, 2019

四、會議地點

華沙/弗次瓦夫(Novotel Wrocław Centrum)

五、會議議程

SA3 #96 會議議程如下：

1	Opening of the Meeting
2	Approval of Agenda and Meeting Objectives
3	IPR Anti-Trust Law and other Reminders
4	Meeting Reports
5	Items for early consideration
6	Reports and Liaisons from other Groups
7	Work Areas
7.1	Security aspects of 5G System - Phase 1
7.2	Security Assurance Specification for 5G
7.3	eMCSec R16 security
7.4	Security aspects of single radio voice continuity from 5GS to UTRAN
7.5	Enhancements for Security aspects of Common API Framework for 3GPP Northbound APIs
7.6	Security of URLLC for 5GS
7.7	Security for 5GS Enhanced support of Vertical and LAN

	Services
7.8	Security of Cellular IoT for 5GS (CIoT_sec_5G)
7.9	Security of the Wireless and Wireline Convergence for the 5G system architecture
7.10	Security aspects of Enhanced Network Slicing
7.11	Other work areas
7.12	New work item proposals
8	Studies
8.1	Study on Security Aspects of the 5G Service Based Architecture
8.2	Security aspects of single radio voice continuity from 5G to UTRAN
8.3	Study on authentication and key management for applications based on 3GPP credential in 5G
8.4	Study on evolution of Cellular IoT security for the 5G System
8.5	Study on the security of the Wireless and Wireline Convergence for the 5G system architecture
8.6	Study on Security Aspects of PARLOS
8.7	Study on 5G security enhancement against false base stations
8.8	Study on Security aspects of Enhancement of Network Slicing
8.9	Study on Security of the enhancement to the 5GC location services
8.10	Study on security for 5G URLLC
8.11	Study on SECAM and SCAS for 3GPP virtualized network products
8.12	Study on Security for 5GS Enhanced support of Vertical and LAN Services
8.13	Study on LTKUP Detailed solutions
8.14	Study on User Plane Integrity Protection
8.15	Study on Security Impacts of Virtualisation
8.16	Study on authentication enhancements in 5GS
8.17	Study on Security for NR Integrated Access and Backhaul
8.18	Study on Security Aspects of 3GPP support for Advanced V2X Services
8.19	Other study areas
8.20	New study item proposals
9	Work Plan and Rapporteur Input
10	Future Meeting Dates and Venues

11	Any Other Business
12	Close

會議進行之時間安排如下：

Monday

- Agenda items 1 – 4
- 9.1 Review of work plan
- 6. Reports and Liaisons from other Groups
- 5. Items for early consideration
- 7. Work areas

Tuesday

- 7. Work areas
- 7.9 New work item proposals
- 8.20 New study item proposals
- 8. Studies

Wednesday

- Handling of revised and outgoing documents
- 7. Work areas
- 8. Studies

Thursday

- Handling of revised and outgoing documents
- 8. Studies

Friday

- Handling of revised and outgoing documents
- 8. Studies
- 9.2 Update of work plan
- Agenda items 10 – 12

後續會議時間與地點如下：

Meeting	**Date**	**Location**

2019		
SA3#97	18 - 22 November 2019	Reno, Nevada, USA
2020		
SA3#98	10 – 14 February 2020	China
SA3#99	11 – 15 May 2020	Dubrovnik, Croatia
SA3#100	13 – 14 July 2020	TBD
SA3#101	02– 06 November t 2020	TBD

六、會議紀要

本次會議由European Friends of 3GPP主辦，包含：Deutsche Telekom、Ericsson、Huawei、Intel、Nokia、Orange、Qualcomm、TIM、Apple等公司，此次會議約有200人與會。本計畫團隊依規劃有1位成員出席參加會議

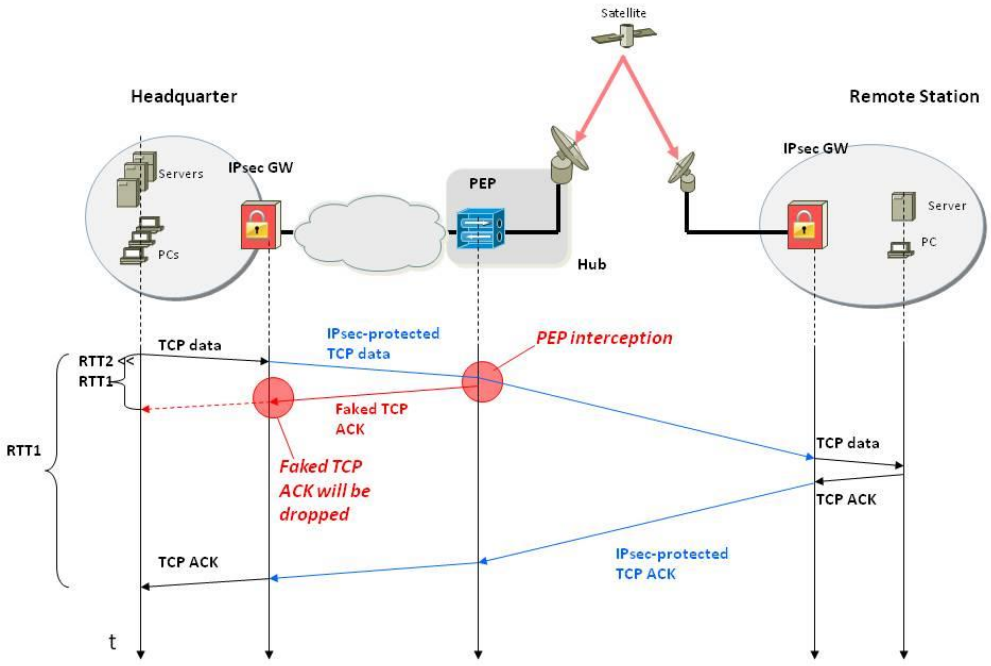
- **Security for Satellite Backhaul**
  - S3-192517 Issues with encryption of satellite backhaul, TNO, Avanti Communications Ltd, VT iDirect Solutions Ltd, ICS

傳統上認為回程連接（Backhaul）- 即無線存取網路(Radio Access Network, RAN)和核心網路(Core Network, CN)之間的連接- 在很大程度上超出了 3GPP 的範圍。它通常被認為是底層傳輸網絡的一部分，因此預期會提供正常 3GPP 操作所需的所需帶寬和服務質量。當衛星連接提供回程連接時，這些假設並不總是適用。例如，衛星回程可能無法支持低延遲。除了上述帶寬和服務質量方面，衛星連接還需要注意安全性，如本討論文件所示。

在 3GPP TS 33.501 規格中，規定 RAN 和 CN 之間的回程網路

應保密（和完整性）。沒有規定應使用網際網路安全協定(Internet Protocol Security, IPsec)技術，但一般產業共識 5G 和 4G 網絡必須支持 IPsec，因此也都建議使用 IPsec 作為行動網路之回程連接。

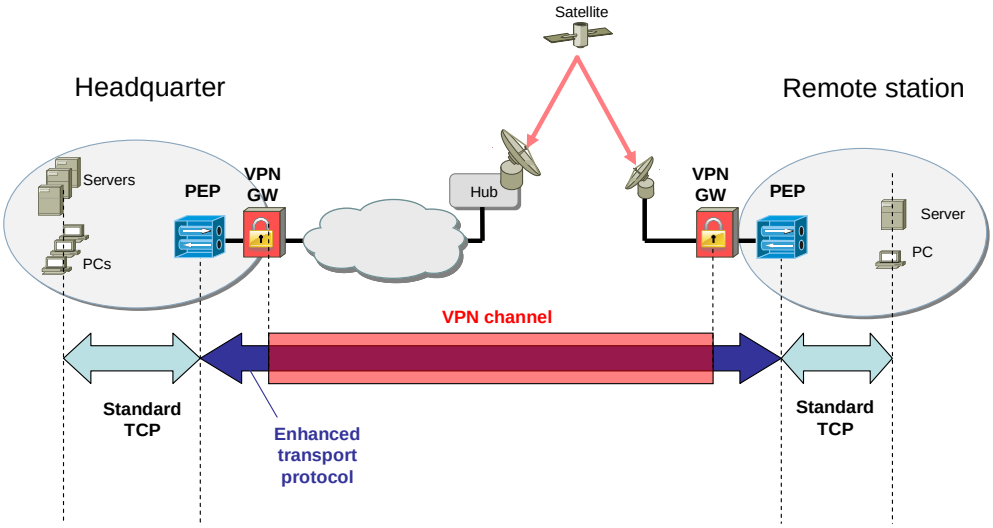
但若使用衛星作為回程連接時，使用 IPSec 可能就有問題。原因主要是衛星鏈路的時延通常很大，無法像固網回程網路做到低時延，因此在衛星鏈路中通常會使用效能增強代理器(Performance Enhancing Proxies, PEP)如下圖:



衛星鏈路 PEP 在端到端 IPSec 環境

在該圖中顯示了使用 IPsec 進行完整性保護對於 PEP 的用戶來說是有問題的。這是因為對於端到端 IPsec 連接，使用 PEP 是有問題的：因為 PEP 在網際網路通訊協定(Transmission Control Protocol, TCP)連接上運行，而 IPsec 封裝（和加密）在 TCP 內部隧道(Tunnel)內。

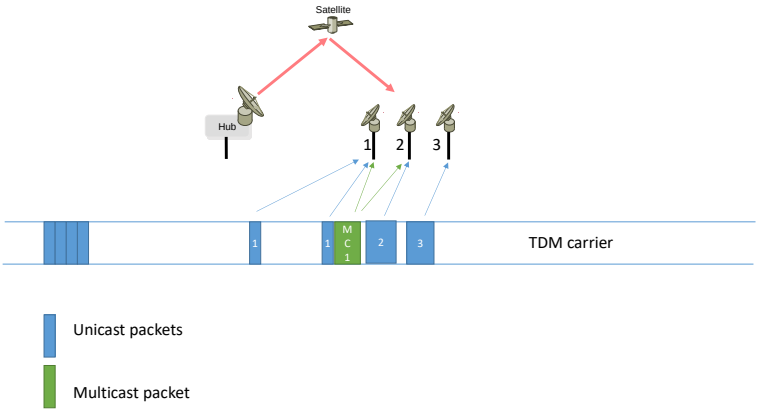
針對以上問題的可能解法之一是採用下圖虛擬私有網路(Virtual Private Network , VPN)的作法，將 PEP 放在 IPsec 隧道外。然而，下圖所示的將 PEP 與 IPsec 結合使用的解決方案不符合 3GPP



PEP 放在 IPsec 隧道外

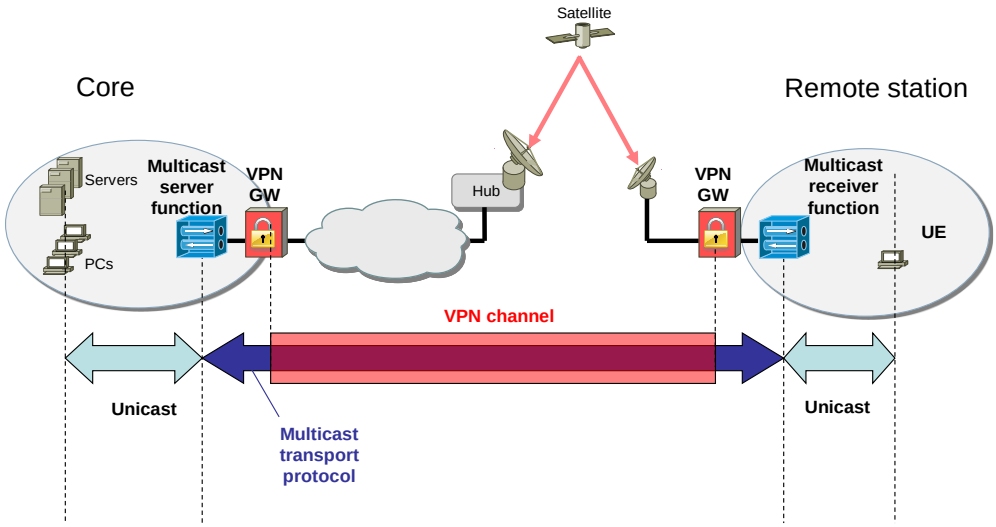
要求 RAN 和 CN 之間的連接應受到機密性保護，除非在上述 IPsec 使用之外採取其他安全措施。

在衛星鏈路向僅支持單播流量的向前傳輸 RAN 提供回程服務的情況下，可以實現（虛擬或物理）多播接收器功能，其將有效衛星多播轉換為本地單播流量，參見下圖。



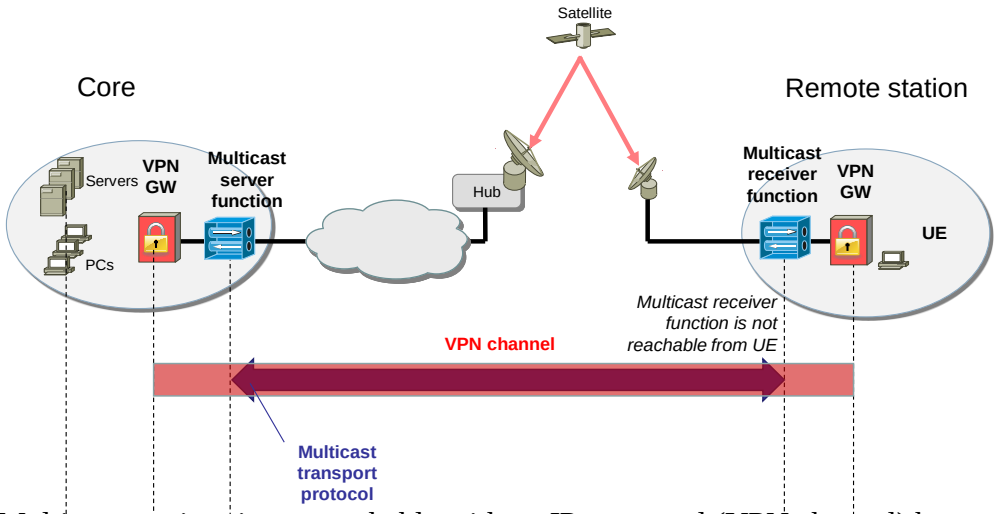
Implementing multicast over a TDM forward satellite link channel

在這種情況下，可以在多播服務器功能和多播接收器功能之間應用 IPsec，但在這種情況下，它將干擾衛星多播功能(如下圖)，特別是



IPsec tunnel (VPN channel) interferes with multicast over satellite

將加密的多播流量分別發送到每個衛星終端，從而否定了衛星多播的好處。更糟糕的是 IPsec 連接應用於多播設置的“外部”，即流量在進入多播服務器功能之前被加密的情況(如下圖)。



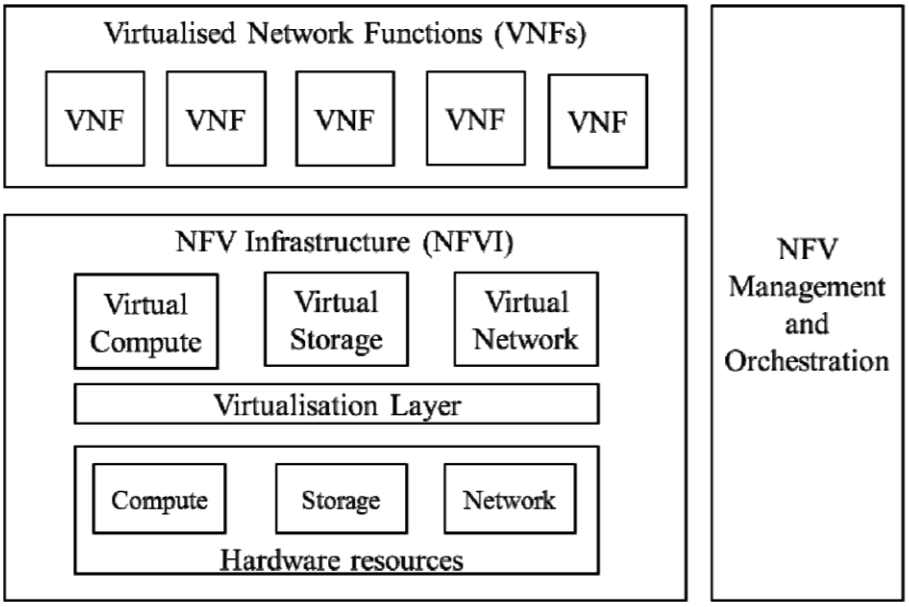
Multicast receiver is not reachable with an IPsec tunnel (VPN channel) between Remote station and Core

另外當 5G 在邊緣計算配置的情況下，遠程站點的本地用戶面功能(User Plane Function , UPF)連接到中心位置的中央 UPF，此處也可以應用本地 UPF 和中央 UPF 之間的 IPsec 來提供安全性。然而，這種情況類似於上述衛星鏈路會發生的安全議題情況。

基於以上的原因，本提案建議在 3GPP SA3 中啟動一研究項目，研究在 3GPP 網絡中使用衛星連接的上述安全方面（以及可能的其他方面）。

- **Security for NFV**
  - S3-192543 TR 33.848 Clarifications for Section 4, NCSC

由於網路功能虛擬化(Network Function Virtualization, NFV)與雲化是 5G 核心網路的基礎，在廠商實做都會採用以下歐洲電信標準協會(European Telecommunications Standards Institute, ETSI)所訂的 NFV 架構:



ETSI NFV high-level architecture (ETSI GS NFV 002)

5G 的核心網路因為使用 NFV 技術而引進了 4G 沒有的資安議題，需要特別制定方案確保 NFV 技術應用在 5G 的安全。本提案即針對 TR33.848 文件建議增加以下的有關 NFV 技術安全應用的相關描述:

- 添加了一個註釋，即容器和虛擬機監控程序在架構描述中不提供相同的安全屬性。

- 雖然可以比虛擬主機的某些漏洞更好地理解物理主機的某些漏洞，但它們不一定容易防範。
- 介紹說明完全虛擬化與有限虛擬化的優勢。

■ **Security for Protection of System Information**

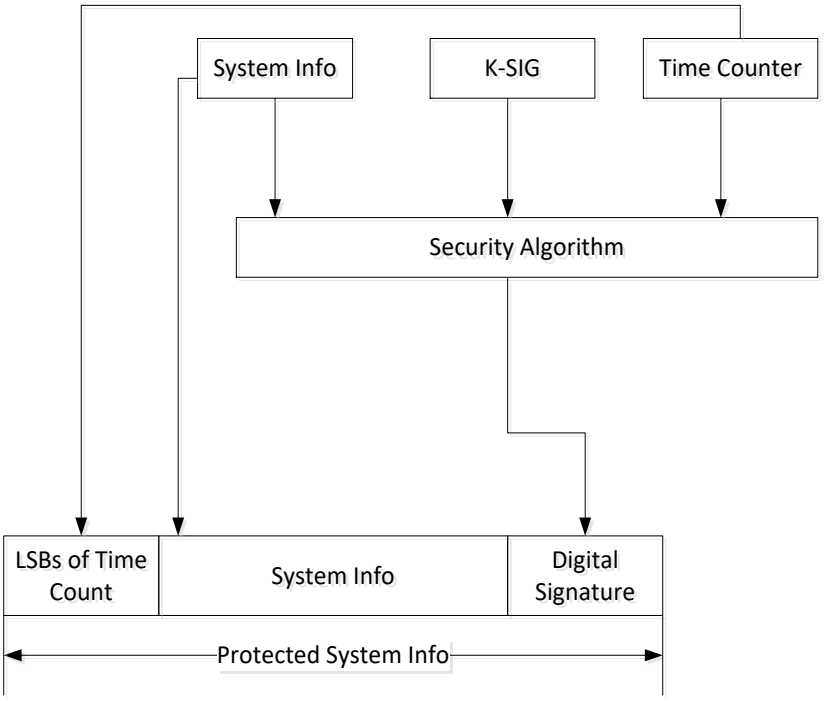
- S3-192638 pCR: Update for solution #7, Apple

網路的系統信息 (System Information)是網路重要參數的廣播平台，所有用戶終端都要靠系統信息獲得網路重要參數進而才能接入系統；從另一方面說，系統訊息的安全性需要被特別保護，以免被有心人擷取進而盜入或癱瘓系統。

針對系統信息的安全保護包括以下兩議題:

- 阻斷服務攻擊（Denial-of-Service, DoS）攻擊：試圖阻止用戶終端(User Equipment, UE)訪問網絡。
- DoS 攻擊網絡：試圖阻礙網絡向 UE 提供服務的能力。

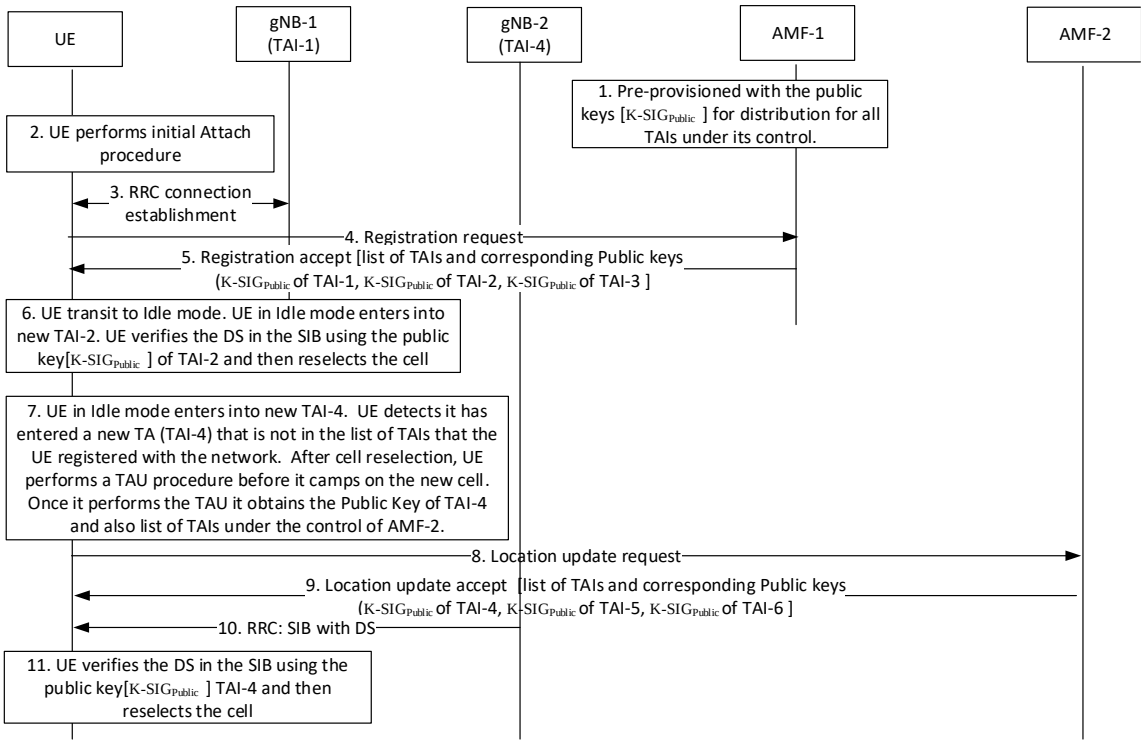
由於細胞(Cell)會周期性地廣播同步信號和系統信息，UE 基於同步信號檢測細胞，如果檢測到的細胞的信號質量高於定義的臨界值，則 UE 確定小區是否真實，駐留在其上如果從細胞接收的系統信息



System Information verification using Digital Signatures

的真實性驗證成功，則細胞是可信的。該解決方案在初始註冊過程期間不驗證細胞的真實性。本提案提出幾個可能解決方案:

第一個是採用數位簽章(Digital Signature, DS)的方案。為了使 UE 能夠驗證所接收的系統信息的真實性，NR 對所廣播的系統信息進行數字簽名，如上圖所示。要廣播的系統信息，私有安全密鑰（K-SIGPrivate）和時間計數器被輸入到安全算法以生成數字簽名。在通過空中傳輸之前，將生成的數位簽章與時間計數器的一些最低有效位一起添加到系統信息中。 K-SIGPrivate 特定於跟踪區域。私有密鑰（K-SIGPrivate）由電信運營商在基站中提供。當執行位置更新過程時，公共 K-SIG 公共密鑰及其生存期由核心網絡提供給 UE，如下圖所示。時間計數器基於世界協調時間（Coordinated Universal Time, UTC），以 10 毫秒為單位維持 UTC 秒數，基站基於



Provisioning of Public Keys to the UE

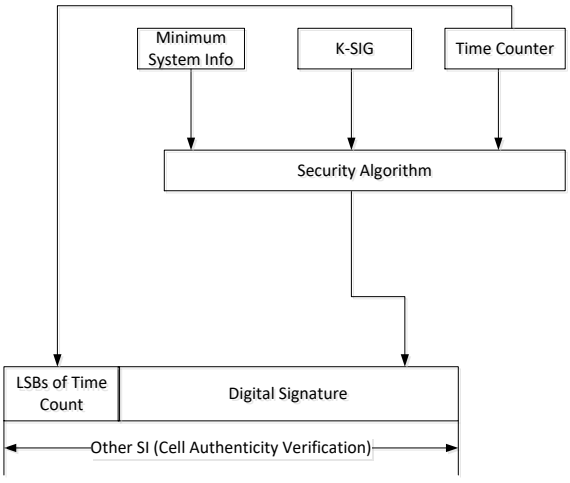
UTC 時間獲得與傳輸時隙相關聯的基於 UTC 的計數器的值。 UE 可以從任何可用的源獲得 UTC 時間，例如 RAN 的系統信息。安全算法的時間計數器輸入是對應於發送系統信息的時隙的計數器的

值。時間計數器的使用確保無法重播收到的系統信息。由於不同的 UTC 源或實現錯誤，UE 和接入網中維持的時間計數器可能存在差異。為了處理這些錯誤，時間計數器的最低有效位也與系統信息一起傳輸。

在接收系統信息時，UE 生成數字簽名。接收到具有數字簽名的系統信息，公共安全密鑰（K-SIGPublic）和接收系統信息的時隙的時間計數器用於檢查 SI 的真實性。如果真實性驗證成功，則係統信息是可信的，並且 UE 認為該細胞是可信的。

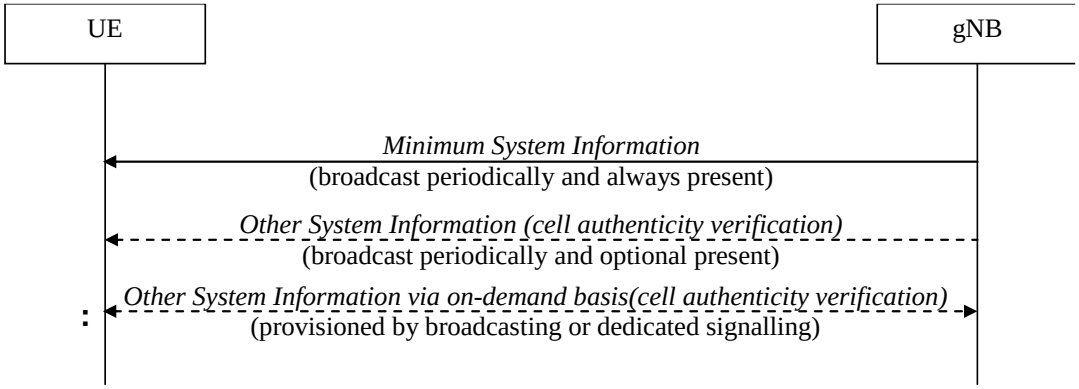
數字簽名的大小導致信令開銷的增加。為了減少開銷，可以一起為多個系統信息生成數字簽名，而不是為每個系統信息生成數字簽名。定期廣播系統信息，以減少開銷;保護可以在每個“N”時段而不是每個時段應用一次。

第二個是採用基於身份加密的的方案。網絡為 UE 和 NR 提供一組用於基於身份的加密的基於橢圓曲線無證書籤名憑證（Elliptic Curve- based Certificateless Signatures for Identity-based Encryption , ECCSI）。此外，UE 被提供有特定於每個小區的公共驗證令牌，並且 NR 配置有與其小區標識相關聯的秘密簽名密鑰。為了驗證小區的真實性，NR 充當“簽名者”並且 UE 充當“驗證者”。 NR 使用與小區相關聯的秘密簽名密鑰來簽署系統信息，並且 UE 使用 CN 的公鑰和小區識別特定公共驗證令牌來驗證簽名。



Cell authenticity verification using other SI

5G 系統信息(System Information, SI)分為最小 SI 和其他 SI。其他 SI 可以由基站廣播或以專用方式提供，由網絡觸發或者根據 UE 的請求觸發。真實性驗證信息可以被分類為其他 SI。 基站生成具有最小 SI 廣播的數字簽名，私有安全密鑰（K-SIGPrivate）和時間計數器作為輸入（如上圖所示），並在其他 SI 中提供數字簽名（作為單獨的 SI） 週期性地或根據 UE 的請求（如下圖所示）。由於 UE 需要驗證基站的真實性，因此僅執行最小 SI 的簽名以便減少 UE 和基站中的開銷。

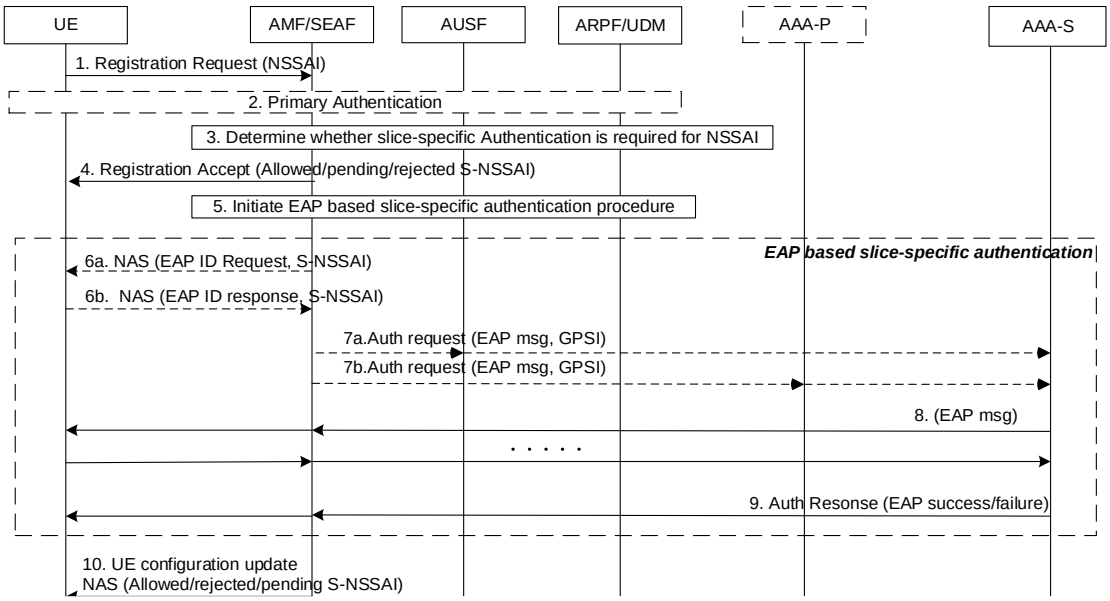


Transmission of cell authenticity verification using other SI

- **Security for Network Slicing**
  - S3-192726 EAP based slice-specific authentication, Huawei, HiSilicon

網路切片(Network Slicing)是 5G 的重要技術，因網路切片的實現多依賴雲(Cloud)以及網路功能虛擬化(Network Function Virtualization, NFV)等軟體化技術，額外引進了資安的議題。

本提案建議一種擴展認證協議（Extensible Authentication Protocol，EAP）的網路切片間認證機制，指定 UE 和認證授權與計費(Authentication Authorization Accounting, AAA)服務器之間可選的使用切片特定認證。整個認證流程如下圖:



Slice-specific authentication procedure

UE 向一個或多個單網路切片輔助選擇資訊(Single Network Slice Selection Assistance Information, S-NSSAI)發送註冊請求以啟動註冊過程，接入移動管理功能(Access and Mobility Management Function, AMF)應根據本地或統一數據管理(Unified Data Management, UDM）存儲的信息確定每個 S-NSSAI 是否需要特定於片的認證。例如，如果基於訂閱信息不需要切片特定認證，則 UE 先前已成功執行切片特定認證並且結果仍然有效，或者針對 UE 的切片特定認證通過不同的訪問類型的方式。AMF 可以向 UE 發送包括在非接入層（Non-Access Stratum, NAS）消息的 EAP 容器中的 EAP ID 請求。相應的 S-NSSAI 也包含在 NAS 消息中。 NAS 消息受安全保護（加密且受完整性保護）。AAA-S 必須向 AMF 發送認證結果。如果不成功，EAP 消息中的 EAP 失敗將發送到 AMF，也可能會將原因發送到 AMF。如果成功，EAP 消息中的 EAP 成功發送到 AMF，則認證的有效期也可以發送到 AMF。 AMF 在本地存儲結果或發送到 UDM 以供將來使用。AMF 應發送 UE 配置更新，以根據特定於切片的認證結果更新所請求的 S-NSSAI 狀態。如果 S-NSSAI 的切片定認證失敗，則拒絕的 NSSAI 與原因一起更新。

如果針對 S-NSSAI 的切片認證成功，則允許的 NSSAI 與有效時段一起更新。