利用 RPKI 強化路由安全之實作

林書呈
財團法人國家實驗研究院國家高速網路與計算中心
0403130@narlabs.org.tw

論文摘要

隨著科技日新月異，網路已經成為人們生活中不可或缺的一部分，網路使用邊界閘道協定(Border Gateway Protocol, BGP)進行路由資訊交換，達成各 ISP 之間的互連。由於 BGP 協定的運作屬信任制，近年發生許多駭客散布錯誤路由資訊或網路管理者宣告錯誤路由，造成全球網路骨幹流量異常流動與網路無法連線的狀況，網路業者產生相當大的損失。為解決這個狀況，全球網路註冊管理機構開始推動資源公鑰基礎建設(Resource Public Key Infrastructure, RPKI)這項技術。RPKI 採用公開金鑰基礎建設框架，讓各 ISP 在交換路由時驗證來源的合法性，確保路由安全。本文先介紹 RPKI 的基本原理與發展現況，接著將 RPKI 的技術實作於台灣學術研究網路的骨幹上，驗證技術之可行性，最後總結結論及未來發展之方向。

關鍵詞：邊界閘道器協定、路由安全、資源公鑰基礎建設、路由來源授權

1 前言

網際網路自 20 世紀開始蓬勃發展，利用標準的 TCP/IP 協定，將全世界幾十億個裝置連結起來，形成邏輯上單一的龐大網路。全世界的網路位置由網際網路號碼分配局(Internet Assigned Numbers Authority, IANA)負責掌管，先將網路位置等資源分配給全球五個區域網路註冊管理機構：APNIC(亞太)、ARIN(北美)、AfriNIC(非洲)、LACNIC(拉丁美洲) 、RIPE NCC(歐洲、中東、中亞)，再由這些區域性組織向下分配到各個國家，像是台灣就由台灣網路資訊中心(TaiWan Network Information Center, TWNIC)負責 IP 網路位址以及自治網路號碼(Autonomous System Number, ASN)的配發事務。

全球的網路服務供應商(Internet Service Provider, ISP)或大型組織，必須先向各國的 IP 網路註冊管理機構申請 IP 位址以及 ASN，透過 BGP 協定與其他 ASN 交流，每個 ASN 都是 IP 位址前綴(IP Prefix)的集合，來連結全球網路，讓全世界的 IP 位址可以彼此串接，BGP 在控制路由傳播以及選擇最佳路徑的功能扮演重要的角色。然而 BGP 協定在設計之時，針對路由交換的設定採取信任制，每個自治網路都會無條件的信任 BGP 鄰居發給自己的所有路由宣告，除非自行設定過濾條件，不然所有互連 ISP 交換的路由資料都會送進網路路由設備的路由表中，進而影響網路連線的最佳路徑選擇。

在 2017 年 8 月，Google 對外錯誤宣告了一個屬於日本 ISP 的 IP 位址前綴，送給與 Google 互連的 ISP，造成屬於日本 ISP 的網路流量跑進 Google 網路骨幹後封包被丟棄，造成網路連線中斷，影響日本 ISP 網路的正常連線[1]；在 2018 年 4 月，更有駭客集團惡意宣告 Amazon 的 DNS 網段給互連 ISP，讓 Amazon 的 DNS 流量流向位駭客安裝於俄羅斯的假冒伺服器，趁機竊取了上萬美元的乙太幣，造成 Amazon 用戶的財務損失[2]；另外在 2018 年 11 月，更發生中國挾持 Google 的流量的事件，後來調查後發現是奈及利亞的 ISP 業者錯誤的宣告了 Google 雲端服務的 IP 位址前綴，造成北美連往 Google 的流量一度流向亞洲的中國電信，也一度造成中美兩國關係的緊張[3]；台灣在 2018 年也因為國內某一 ISP 路由宣告錯誤，造成中華電信 Hinet 連線國外網站的服務因為流量轉向該 ISP 而壅塞，經過緊急啟動保護措施後網路服務才恢復。由於 BGP 協定奠基在 ISP 業者之間的互信，近年來不論是惡意的網路攻擊事件或錯誤的路由宣告，已有多起事件影響網路連線，負責網路位址等資源的註冊管理機構陸續提出一些強化路由安全的方法，其中最有效率的解決方式，就是導入資源公鑰基礎建設的技術，本文後續將探討此技術帶來的好處並將 RPKI 實作於台灣的學術研究骨幹上。

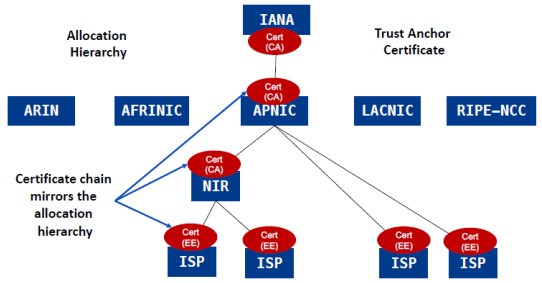
2 RPKI 基本原理與發展現況

現今網路上最常見的路由安全問題，多為 IP 位址前綴宣告錯誤所造成，由於 BGP 協定並無檢查路由來源宣告正確性的能力，導致錯誤宣告的 IP 位址前綴被散播到整個網際網路上，造成嚴重的網路路由安全事故，為解決這樣的狀況，RPKI 的技術應運而生。RPKI 透過簽署認證一種特定格式的數位憑證與簽章，幫助網路路由設備比對 BGP 路由來源宣告訊息的正確性，進而提高 BGP 協定的安全性，降低網際網路路由宣告錯誤事件的發生。

2.1 RPKI 基本原理

RPKI 的中文全名為「資源公鑰基礎建設」，創立的想法是把 IP 位址以及 ASN 兩種網路號碼資源，利用公鑰基礎建設(Public Key Infrastructure, PKI)的框架對所有權進行認證，讓 IP 位址的傳遞能獲得更高的安全性。RPKI 使用 RFC3779 定義的 X.509 授權憑證格式，將 IP 位址以及 ASN 的組合進行簽署，憑證的結構依據網際網路資源的分發方

式，每一個網際網路號碼資源的註冊單位都是憑證授權中心(Certificate Authority, CA)，在註冊單位將IP位址以及ASN配發給下級單位時，同時會簽署一張資源憑證給該單位，以確認這個資源的所有權。



圖一：憑證簽署架構示意圖

(Source: https://www.slideshare.net/apnic/peering-asia-20-rpki-for-peering)

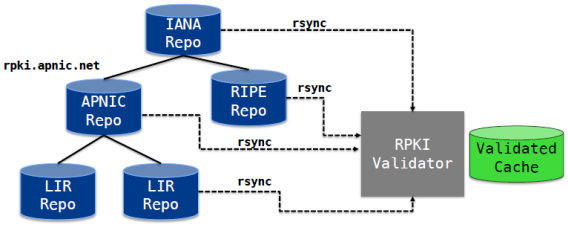
以上圖一來說明整個憑證的簽署過程，所有網路號碼資源由IANA統一分發，所以IANA具有所有號碼資源的憑證，當IANA將號碼資源分配給五個區域網路註冊管理機構(Regional Internet Registries, RIRs)時，也會同時簽署資源憑證給這些RIRs，當RIRs(例如APNIC)再將其資源向下分配給國家網路註冊管理機構(National Internet Registries, NIRs)時，也會同時簽署資源憑證給NIRs，RIRs及NIRs需扮演憑證授權中心的角色。而當ISP或一般大型組織向NIRs或者是RIRs申請IP位址及ASN時，除了獲得號碼資源外，也會獲得經號碼資源註冊單位簽署的終端憑證(End Entities)，經過這樣的過程，資源持有單位都可獲得合法簽署過的憑證資料。

路由起源授權(Route Origin Authorization, ROA)則是用於將IP位址前綴以及ASN進行連結的一個元件，可用來作為加密驗證。資源持有單位如ISP可利用註冊單位簽署過的IP位址終端憑證以及ASN終端憑證進行ROA的建立，讓IP位址前綴與ASN的關係連結起來，單一筆IP位址前綴可以建立多筆ROA。下圖二為ROA的一個範例，代表AS7539這個自治網路已被授權可宣告211.79.48.0/20這段IP位址前綴，且允許接受最大的前綴長度為/24，只要是在/24之內的IP位址前綴都是被授權宣告的，其他的自治網路若宣告這組IP位址前綴就會被視為非法宣告。

Prefix	211.79.48.0/20
Max-length	24
Origin ASN	AS7539

圖二：ROA格式範例

當ROA被建立之後，註冊管理機構就會將一筆一筆的ROA紀錄儲存在當地的資料庫中，ROA是由多個分散是資料庫所儲存，RPKI Validator則是會利用rsync週期性的同步下載這些建立好的加密ROA元件，並儲存一份本地驗證的快取，供網路路由設備連結使用。若網路路由設備啟用RPKI技術，則可將網路路由設備與RPKI Validator建立連結，將ROA元件的資料下載網路路由設備中，供設備進行BGP路由策略決策使用，RPKI Validator資料同步架構如下圖三所示。



圖三：RPKI Validator資料同步架構

(Source: https://www.slideshare.net/apnic/peering-asia-20-rpki-for-peering)

當網路路由設備同步完成本地驗證的快取後，就可以比對路由表中的每一筆IP位址前綴，驗證每一筆IP位址前綴來源宣告的有效性，每一筆IP位址前綴比對來源宣告後有以下三種結果：

- 有效(Valid)：代表該筆IP位址包含在一個ROA元件中，且ASN號碼一致，是來源合法的IP位址宣告。
- 無效(Invalid)：代表該筆IP位址包含在一個ROA元件中，且ASN號碼不一致，表示該筆IP位址的來源位址是沒有獲得授權的，或者是該筆IP位址宣告的前綴長度超過ROA中設定的最大長度。
- 未知(Not found/Unknown)：代表該筆IP位置並未包含於現有的ROA紀錄當中，由於無ROA紀錄可供比對，無法確定其來源宣告的合法性。

當網路路由設備的每一筆IP位址都多了來源宣告驗證的屬性之後，就可以提供BGP協定一個新的路由策略決策依據，讓網路路由設備可以過濾掉狀態為無效的IP位址宣告，或者是調高有效IP位址宣告的優先等級，讓路由安全能夠獲得更好的保障。

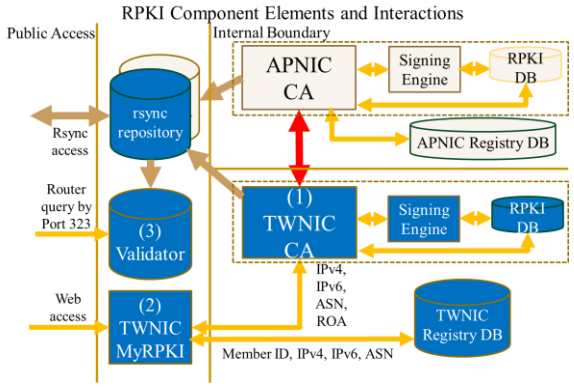
2.2 RPKI發展現況

為推動RPKI技術的普及性，由國際網路標準組織IETF推動將RPKI的技術標準化，以RFC6480定義RPKI的架構，讓各網路路由設備廠商有一共通的標準可以遵循。自2009年起，全球五大RIR開始佈署憑證授權中心和憑證物件管理系統，為下屬的註冊管理機構及資源持有單位簽署憑證，在RIRs完成佈署之後，接著就輪到NIRs需要開始佈署相關的憑證授權中心以及憑證物件管理系統了。

台灣的網路註冊管理機構TWNIC在去年陸續完成憑證授權中心以及憑證物件管理系統的建置，整個系統架構如下圖四所示：

TWNIC CA與APNIC簽署CA憑證，在TWNIC建立一個可信任的憑證授權中心，APNIC會將屬於TWNIC的憑證資源指定給TWNIC，並儲存在TWNIC CA的資料庫中[4]。接著TWNIC PRKI服務管理系統會與TWNIC資源管理系統溝通，取得使用者資料、IP位址、ASN等資源，並與TWNIC CA資料進行比對，TWNIC資源持有單

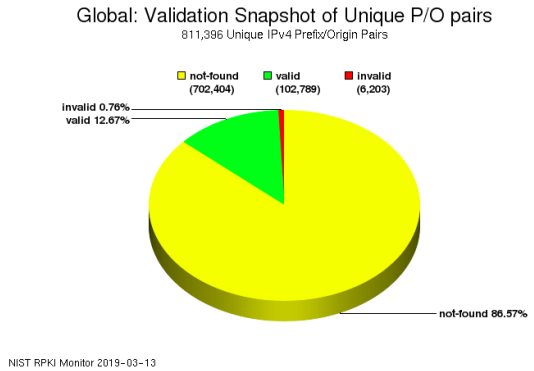
位透過 TWNIC PRKI 服務管理系統檢視其資源憑證及管理(新增/修改/刪除)ROA 元件，並傳到 TWNIC CA 伺服器。TWNIC CA 每日定期透過 rsync 同步到資料庫並加入 APNIC 的信任錨(Trust Anchor)，讓使用者可以透過驗證工具驗證 ROA 設定，並提供 TWNIC RPKI Validator 驗證工具讓使用單位及網路路由設備進行驗證。



圖四：TWNIC RPKI 實作架構

(Source: https://rpki.tw/RPKI_technology.html)

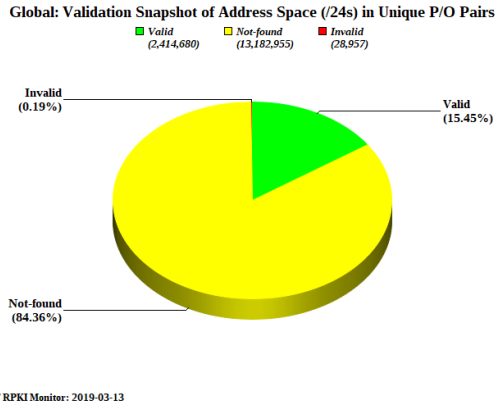
在 RPKI 推動現況統計分析方面，美國國家標準及技術研究院(National Institute of Standards and Technology, NIST)為協助了解 RPKI 技術在全球的推展情形，故開發了 RPKI 監控系統，提供包含全球以及五個區域網路註冊管理機構推行 RPKI 成果的相關統計資料，對了解 RPKI 發展現況有相當大的幫助[5]，以下圖五為例，全球目前被宣告的 IPv4 位址前綴數量約為 81 萬筆，若與全球五個 RIRs 資料庫當中被建立的 ROA 紀錄進行來源宣告驗證，狀態呈現為有效的 IPv4 位址前綴數量約為 10 萬筆左右，佔整體 IPv4 位址前綴總數的 12.67%；狀態呈現為無效的 IPv4 位址前綴數量約為 6 千筆左右，佔整體 IPv4 位址前綴總數的 0.76%；其餘 IPv4 位址前綴比對的結果皆為未知，佔總數的 86.57%，代表目前 RPKI 的實作的比例還有很大的進步空間。



圖五：全球來源宣告驗證結果-依前綴數

(Source: https://rpki-monitor.antd.nist.gov/?p=0&s=0)

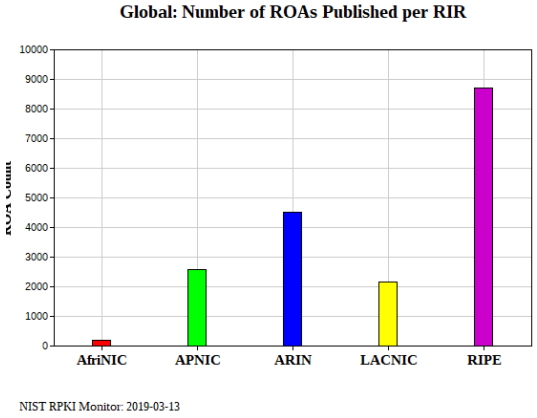
若以前綴長度/24 來估算所有 IP 位址當中實作 RPKI 的比率(參考圖六)，則可算出目前所有 IPv4 位址空間當中，約有 15.45%的 IPv4 位址來源宣告驗證的狀態是有效的，無效的比例約為 0.19%，而未知的比例約為 84.36%，還是佔了大部分的比例。



圖六：全球來源宣告驗證結果-依 IP 數

(Source: https://rpki-monitor.antd.nist.gov/?p=0&s=0)

若我們以全球五大區域網路註冊管理機構資料庫中 ROA 的數量統計來看，可以發現歐洲 RIPE 在推廣 RPKI 的速度與成效是比較好的，ROA 紀錄的數量超過 8000 筆，再來依序是北美洲 ARIN、拉丁美洲 LANIC 以及亞洲 APNIC，非洲因為資訊推行的速度較慢，所以 ROA 紀錄的數量最少。



圖七：各 RIR 建立之 ROA 數量統計

(Source: https://rpki-monitor.antd.nist.gov/?p=0&s=1)

3 RPKI 於學術研究網路之實作

台灣高品質學術研究網路(TaiWan Advanced Research and Education Network, TWAREN)[6]是為學術研究而設的專用網路，服務對象包含國內各大專院校、政府機關及研究單位等，由國家高速網路與計算中心負責網路維運管理。作為台灣的學術研究網路的維運單位，我們向台灣網路註冊管理機構 TWNIC 申請一個自治網路號碼 AS7539，用來與全球學術研究網路單位進行 BGP 路由互連，也向 TWNIC 申請 IPv4 位址與 IPv6 位址作為對外提供連線服務使用，為了強化 TWAREN 網路骨幹的路由安全性，我們在骨幹設備上實作了 RPKI 的技術，並調整路由過濾機制來確保 BGP 路由安全。

3.1 建立路由起源授權

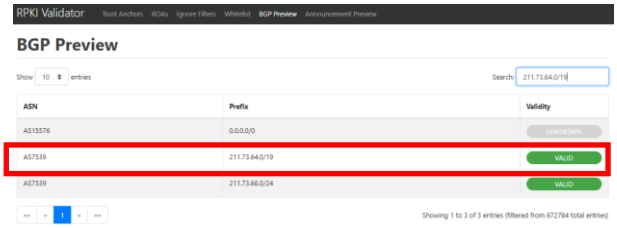
台灣網路資訊中心在 2018 年 10 月將 RPKI 服務系統(https://myrpki.twnic.tw)[7]正式上線，網站提供 IP 持有單位檢視其資源憑證與新增、修

改、刪除路由起源授權元件的功能，只要是向 TWNIC 申請 IP 位址的資源持有單位，都可申請 RPKI 服務系統網站帳號密碼。本中心擁有的 IP 位址以及 ASN 都是向 TWNIC 申請，故本中心也有一組 TWNIC RPKI 服務系統的帳號。

在登入 TWNIC RPKI 服務系統後，可以檢視本中心所申請的 IPv4 位址、IPv6 位址以及 ASN 等資源清單，而左方的功能選單，也提供 ROA 管理的功能，初次登入時系統並無 ROA 紀錄，需自行手動新增，如下圖八所示，我們將申請到的 IPv4 位址以及實際宣告時使用的 ASN 連結在一起，即可建立一筆 ROA 資料。ROA 資料在建立完成後，就會儲存在 TWNIC 的資料庫，並以 rsync 技術定期同步各註冊管理機構建立的 RPKI Validator 伺服器上。

圖八：新增 ROA 範例

TWNIC 也有提供 RPKI Validator 查詢的服務 (https://validator.twnic.net.tw/roas)[8]，在 ROA 建立之後，可以到 RPKI Validator 的網站，查詢一下建立的 ROA 是否已同步到 Validator 上，也可利用網站上的 BGP Preview 的功能，查詢目前宣告的 IP 位址路由經 BGP IP 位址前綴來源宣告比對後，所得到的狀態為何。以本中心目前對外宣告的 IP 位址前綴 211.73.64.0/19 為例，在 TWNIC RPKI Validator 上查詢後的結果如下圖九，狀態呈現為 Valid 表示當網路路由設備啟用 RPKI 設定，即有辦法驗證本中心對外宣告 IP 位址前綴來源，若有其他惡意網路攻擊或錯誤設定的自治系統宣告本中心的 IP 位址前綴，即可利用 BGP 的來源宣告驗證屬性將錯誤的路由宣告過濾，確保網路路由設備的路由安全。



圖九：RPKI Validator 來源宣告比對查詢

3.2 路由驗證之連結與路由過濾

在完成 ROA 的建立之後，接著就要設定網路路由設備與 RPKI Validator 之間的連結，由於 RPKI 是 RFC6480 所定義的網路標準，所以各廠牌的網路設備大多都有支援 RPKI 的功能，例如 Cisco 使用 IOS-XR 作業系統的網路路由設備，版本在 XR4.3.2 版之後，設備即支援 RPKI；使用 IOS-XE 作業系統的設備，版本在 XE3.5 版之後，都可支援 RPKI 的設定。Juniper 的網路路由設備只要作業系統在 JunOS 12.2 版之後也都有支援 RPKI，其他像是 Quagga 的網路路由設備，也利用 BGP-SRX 技術來支援 RPKI 的設定，相關的設定範例，可參考 RIPE NCC 所提供的參考範例[9]。

```
RPKI cache-servers configured: 1
RPKI global knobs
  Origin-AS validation is ENABLED globally
  Origin-AS validity WILL NOT affect bestpath selection globally
  Origin-AS validity signaling towards iBGP is DISABLED globally
RPKI database
  Total IPv4 net/path: 62409/66427
  Total IPv6 net/path: 10863/11882
```

圖十：RPKI 設定完成之狀態

我們在取得 TWNIC 建置的 RPKI Validator IP 之後，依照範例建立與 RPKI Validator 的連結關係，就可從 RPKI Validator 中獲得 ROA 元件的快取資料，設定完成之後的狀態如上圖十，可看到目前我們已從 TWNIC RPKI Validator 中同步到 62409 筆 IPv4 ROA 紀錄以及 10863 筆 IPv6 ROA 紀錄到網路路由設備來，可供比對 IP 位址的前綴來源使用。當我們在查詢 IP 位址的路由時，設備會比對 ROA 紀錄並將來源宣告驗證屬性新增到路由資訊中，如下圖十一中所示 。

```
BGP routing table entry for 41.60.0.0/20
Versions:
  Process           bRIB/RIB  SendTblVer
  Speaker          919804853   919804853
Last Modified: Aug  8 14:05:21.505 for 1y31w
Paths: (5 available, best #1)
  Advertised to update-groups (with more than one peer):
    1.9 1.12
  Advertised to peers (in unique update groups):
    211.73.77.225   211.79.63.50
  Path #1: Received by speaker 1
  Advertised to update-groups (with more than one peer):
    1.9 1.12
  Advertised to peers (in unique update groups):
    211.73.77.225   211.79.63.50
  3462 4809 30844 37146
    211.20.206.214 from 211.20.206.214 (220.128.33.226)
      Origin IGP, localpref 100, valid, external, best, group-best
      Received Path ID 0, Local Path ID 0, version 919804853
      Origin-AS validity: valid
```

圖十一：路由資訊屬性呈現範例

在網路路由設備啟用 RPKI 之後，我們針對 BGP 路由的屬性，就多了 IP 位址前綴來源宣告驗證的欄位，可以作為與 BGP 鄰居之間路由過濾的參考條件。在路由策略的應用上，首先我們將 IP 位址前綴來源宣告狀態為無效(Invalid)的 BGP 路由過濾，這類路由宣告來自不合法或錯誤的來源 ASN，接著我們針對幾個重要的且已導入 RPKI 的自治網路單位，例如 Google(AS1659)、Microsoft(AS8075)、Facebook(AS32934)、Amazon(AS16509)等，若這些 IP 位址前綴來源宣告狀態為有效(Valid)，就增加路由的優先順序，讓已取得 RPKI 驗證的路由有較高的優先等級。

4 結論與未來展望

鑑於路由錯誤宣告及路由挾持事件日益嚴重，網路基礎架構已成為駭客的攻擊目標，全球主要網路註冊管理機構與網路設備廠商積極推動 RPKI 這項技術標準，提供安全的方法來認證網路

號碼資源的分配，防止路由挾持或其他攻擊，確保路由安全性。TWAREN 提供台灣學術界先進的網路技術研究平台，非常適合新技術的導入，本次將 RPKI 技術實作於 TWAREN 骨幹上，就是希望能夠實際驗證 RPKI 修補現行 BGP 協定無法進行來源宣告驗證的弱點。在實作 RPKI 之後，我們已具備 IP 位址前綴來源宣告比對的能力，可在骨幹網路邊界路由設備上，對 BGP 協定送進的路由進行過濾，把錯誤宣告或惡意挾持 IP 位址前綴的狀況排除，由於目前全球自治網路單位導入 RPKI 的比例還太低，80%以上的 IP 位址前綴來源宣告比對結果都屬於未知，網路路由設備目前僅能針對特定較重要的自治網路搭配來源宣告比對結果進行過濾，尚無法單一利用 IP 位址前綴來源宣告比對來進行過濾，全世界的網際網路是透過無數的自治網路彼此交換路由達成互連，這部份需要全球自治網路導入 RPKI 技術的比率變高後才可改善，RPKI 技術的推廣還需繼續努力。

誌謝

感謝台灣網路資訊中心(TWNIC)積極推動 RPKI，除建立服務系統協助驗證來源路由，也舉辦多場說明會與教育訓練推廣 RPKI，讓台灣的 IP 使用者可以了解此技術的優點並應用在既有的網路設備上。

參考文獻

[1]Google 錯誤宣告日本 ISP 網段事件
https://dyn.com/blog/large-bgp-leak-by-google-disrupts-internet-in-japan/
[2]Amazon DNS53 網路攻擊事件
https://blog.cloudflare.com/bgp-leaks-and-crypto-currencies/
[3]奈及利亞錯誤宣告影響 Google 流量
https://blog.thousandeyes.com/internet-vulnerability-takes-down-google/
[4]TWNIC RPKI 介紹網站 https://rpki.tw
[5]RPKI 全球佈署狀態統計
https://rpki-monitor.antd.nist.gov
[6]台灣高品質學術研究網路
http://www.twaren.net/
[7]TWNIC RPKI 服務系統網站
https://myrpki.twnic.tw
[8]TWNIC RPKI Validator 網站
https://validator.twnic.net.tw/roas
[9]Router 啟用 RPKI 設定指令
https://www.ripe.net/manage-ips-and-asns/resource-management/certification/router-configuration