TWISC@NCTU

TWISC@NCTU

交大資通安全研究與教學中心

DNSSEC 技術評估報告

版本： 1.0

TWISC@NCTU 主任：謝續平教授

參與人員：曾子建、洪凱峰、陳柏愷

本研究成果由教育部補助

目錄

1. 前言 1

2. DNSSEC 標準與最新趨勢研究 3

2.1. 各國的發展及佈署情況 3

2.2. 標準研究 4

2.3. 支援的軟體 6

3. DNSSEC 入門簡介 11

3.1. DNSSEC 運作概要 12

3.2. DNSKEY 紀錄 13

3.3. RRSIG 紀錄 14

3.4. NSEC 紀錄 15

3.5. DS 紀錄與信任鍊（CHAIN OF TRUST） 16

4. DNSSEC 與憑證相關技術研究 19

4.1. SECURE E-MAIL 19

4.2. IP SECURITY（IPSEC） 22

4.3. TRANSPORT LAYER SECURITY（TLS） 22

4.4. 結論 23

5. DNSSEC 與 IPV6 相關技術研究 24

5.1. IPV6 簡介 24
5.2. IPV6 位址表示 25
5.3. IPV6 的特色.....25
5.4. IPV6 與 DNS.....26
5.5. IPV6 與 DNSSEC 27
5.6. 結論 29
6. DNSSEC 與中文網域名稱相關技術研究 31
6.1. 國際化域名（IDN) 31
6.2. 異體中文域名.....32
6.3. IDN 標準帶來的影響與對應解決方法.....33
6.4. INTERNATIONALIZED COUNTRY CODE TOP-LEVEL DOMAIN 35
6.5. DNSSEC 與中文域名相容性.....35
6.6. 結論 36
7. DNSSEC 網路測試實驗室建置.....37
8. 結語.....39

圖目錄

圖 1　Firefox 支援 DNSSEC 9

圖 2　Thunderbird 支援 DNSSEC 10

圖 3　Chain of trust in DNSSEC 12

圖 4　wormhole.movie.edu 的 RRSIG 紀錄 14

圖 5　DNSSEC 架構與 S/MIME 結合後的運作流程圖 21

圖 6　IPv6 對於 DNSSEC 相容性實驗環境 27

圖 7　原 named.conf 部分設定 34

圖 8　轉換後之 named.conf 部分設定 34

圖 9　原 zone file 設定 34

圖 10　轉換後之 zone file 設定 34

圖 11　DNSSEC 實驗平台架構 37

圖 12　DNSSEC 實驗室實況 38

表目錄

表 1　Windows 7 對 DNSSEC 的支援性 7

1. 前言

DNS 可說是目前網路上最重要也最普及的基礎建設之一，幾乎所有的網路應用，包含台灣學術網路 TANet 上的許多應用，都透過 DNS 來將網域名稱解析為 IP，再進行後續的網路連線動作。而近年相當熱門的雲端運算(Cloud Computing)，DNS 的應用也扮演相當重要的角色。傳統 DNS 系統的設計上，並沒有考量到安全強化的問題，因此許多 DNS 攻擊技術相繼被開發出來，並實際被駭客利用。如 2010 年 1 月，中國大陸最大的搜尋引擎公司百度，即受到 DNS 攻擊，導致許多客戶被導向一個惡意的網站。同樣地，台灣學術網路 TANet 也是駭客最活躍的網域，也常遭受 DNS 攻擊，例如交大、台大、成大都曾發生，深受其害。

DNSSEC 為 DNS 的安全強化延伸標準，雖然標準化的工作持續在進行中，初步的標準也才訂定不久，也仍有許多部分付諸闕如，例如 client 到 recursive DNSSEC 伺服器間的認證目前尚未訂定。但因應網路上的大量攻擊事件，對於 DNSSEC 服務需求具有時間上的急迫性，因此根網域（root domain）及許多頂級網域管理機構(如 .org, .net)、國家頂級網域如美國（.us）、日本(.jp)、澳洲(.au)、新加坡(.sg)等已經陸續開始推廣 DNSSEC；預期在幾年內，國際上的 DNS 將陸續升級為 DNSSEC，以提供更好的網路安全性。台灣的 TWNIC 則預期 100 年度下半年將開始建構 DNSSEC 伺服器。

在根網域與國家網域或許可以投入大量資源逐漸建構 DNSSEC 伺服器，但上層網域導入 DNSSEC 後，僅有上層的網域 DNSSEC 伺服器是不夠的，其下層的 DNSSEC 伺服器如何能安全、容易的建置，這將是極大的挑戰。對台灣學術網路 TANet 的各級學校、區網中心而言，缺少高級研發人員，導入 DNSSEC 卻是個需要大量人力與資源的浩大工程，實在力有未逮。為了降低各計算機中心的導入技術門檻與減輕人力與資源負擔，本計畫以 DNSSEC 先期技術研究及系統規劃開發為主，研究開發可輕易快速安裝之 DSNSEC 伺服器端軟體，探討大量建置 DNSSEC

伺服器以及 infrastructure 可能遇到的困難與障礙。此研究成果將可提供教育部參考，做為未來大量導入 DNSSEC 至教育部相關網域（.edu.tw）的先期研究與規劃，為大規模佈署預作準備工作。

本文件包含了 DNSSEC 相關資料，及本計畫團隊在計畫執行期間的測試與研究。內容包括 DNSSEC 最新趨勢與資料收集、DNSSEC 入門簡介、DNSSEC 與憑證相關技術實驗研究、DNSSEC 與 IPv6 相關技術實驗研究、DNSSEC 與中文網域名稱相關技術實驗研究、及 DNSSEC 實際架設情形介紹。

DNSSEC 最新趨勢與資料收集可以幫助我們對於 DNSSEC 後續發展做較正確的應對。DNSSEC 入門簡介可以使讀者更容易對 DNSSEC 上手。DNSSEC 與憑證相關技術實驗研究可以更深入的探討其安全性強度，並研究其弱點與破解的可能性。DNSSEC 與 IPv6 相關技術研究並做更進一步的測試，釐清目前兩者的相容性，以及目前軟硬體的實作情況，作為後續研究開發的參考。DNSSEC 與中文網域名稱相關技術實驗研究考慮到升級到 DNSSEC 之後的相容性問題，確保中文網域名稱能正確使用。

2. DNSSEC 標準與最新趨勢研究

由於 DNSSEC 是相當新穎的技術，收集目前最新的趨勢及佈署狀況有助於我們了解DNSSEC在TCP/IP網路上的重要性。收集支援 DNSSEC 的軟體有利於研究上的便利性同時也可以知道應用程式對 DNSSEC 做了哪些應用。對 DNSSEC 這樣年輕的協定來說，我們能取得的現有軟體在各方面實作未必能完全符合，為了要排除後續開發與佈署上的問題，有必要對協定作足夠的瞭解。

2.1. 各國的發展及佈署情況

目前根網域（root domain）13 台伺服器已經完全支援 DNSSEC，在頂級網域（Top-Level Domain, TLD）方面，目前已經有 9 個已經支援 DNSSEC，較重要的如.net 網域及.org 網域已經支援，而.com 網域已經在實階段，將在 2011 年 3 月正式營運 DNSSEC。

在國家網域方面（Country Code Top-Level Domains, CCTLD），目前有 38 個國家網域已經支援 DNSSEC，較重要的如巴西（.br）、美國(.us)、澳洲（.au）、日本（.jp）、新加坡（.sg）、泰國（.th）、法國（.fr）、英國（.uk）等。

我們從我們觀察到的現象，發現近一年來各網域導入 DNSSEC 的狀況相當踴躍。由於 DNS 是重要的基礎建設，所以升級成 DNSSEC 必須非常謹慎而不能出錯，我們看到大部分的頂級網域都從 2009 年開始實驗，經過一年以上的實驗期才正式導入。由目前實驗中的網域看來，可以預期許多的網域也將陸續在 2011 年正式導入 DNSSEC 維運。

而在台灣，主管.tw 網域的 TWNIC 組織，目前已經開始實驗 DNSSEC，預期在 2011 年將正式導入維運，不過僅有上層的網域 DNSSEC 伺服器是不夠的，且台灣學術網路 TANet 也是駭客最活躍的網域之一， 因此本計畫為協助教育

部相關網域（.edu.tw）導入 DNSSEC 的先期研究與規劃，大規模佈署預作準備工作。

關於各頂級網域支援 DNSSEC 的最新狀況，可在以下兩個網址查詢。

http://en.wikipedia.org/wiki/List_of_Internet_top-level_domains

https://www.dnssec-deployment.org/wp-content/uploads/2010/08/TLD-deployment-Table-8_30_10.pdf

2.2. 標準研究

由於 DNSSEC 是相當新穎的技術，相關文件及實作經驗較少，其中較重要的文件為關於 DNSSEC 的 RFC，此部分 RFC 約有 37 篇，我們選擇核心的數篇加以研究，必要時對照相關 RFC 已建置 DNSSEC 平台。

2.2.1. RFC 4033 - DNS Security Introduction and Requirements

這份文件介紹這些延伸性並描述他們的功能及限制。說明了 DNSSEC 增加了資料來源驗證性（Data Origin Authentication）及資料完整性（Data Integrity）並且也討論 DNSSEC 所不提供的服務，像是保密性（Confidentiality）以及抵抗 Denial of Service Attacks 的能力。

2.2.2. RFC 4034 - Resource Records for the DNS Security Extensions

這份文件說明 DNSSEC 是一堆修改過的協定(Protocol)及資源紀錄(Resource Record)的集合，這集合為 DNS 提供了來源驗證(Source Authentication)的功能。這份文件定義了 Public Key（DNSKEY）、Delegation

signer（DS）、Resource Record Digital Signature（RRSIG）以及 Authenticated Denial of Existence（NSEC）Resource Records。每種資源紀錄的目的以及格式都有詳加描述並且針對每種資源紀錄都有給一個範例。

2.2.3. RFC 4035 - Protocol Modifications for the DNS Security Extensions

此份文件主要在講述 DNSSEC 協定的修改，並定義了簽署 Zone 的觀念還有 DNSSEC 提供服務及解析的所需條件。這些技術使得 Security-Aware Resolver 可以驗證 DNS 資源紀錄及 Authoritative DNS Error Indications。

2.2.4. RFC 5155 - DNS Security (DNSSEC) Hashed Authenticated Denial of Existence

Domain Name System Security（DNSSEC）Extensions 引進了 NSEC 資源紀錄(RR)來驗證 Denial of Existence。之後也引進了 NSEC3，除了擁有 NSEC 的功能之外，也提供了對抗 Zone Enumeration 的方法並允許 Delegation-Centric Zone 的逐步增加。

2.2.5. RFC 4310 - Domain Name System （DNS）Security Extensions Mapping for the Extensible Provisioning Protocol（EPP）

此文件在描述 Extensible Provisioning Protocol（EPP）Extension 對應 Domain Name System Security Extensions（DNSSEC）將 Domain Name 放在中央共儲存裝置上的提供及管理。此種指定在 XML 上的對應關係將 EPP Domain Name 做個延伸，使其可以對應到 DNSSEC 所要求的額外功能。

2.2.6. RFC 4641 - DNSSEC Operational Practices

這份文件是說明 DNSSEC 一些實務上的操作。主要就操作方面在DNS上使用金鑰跟簽章,包括金鑰的產生、金鑰的儲存、簽章的產生、Key Rollover 以及相關的規

則。

2.3. 支援的軟體

除了做文件的研究外，在另一方面我們實做 DNSSEC 平台，在此平台上實做關於 DNSSEC 網路測試實驗室環境以供開發及實驗部分，並試用各項支援 DNSSEC 軟體。由於現在支援 DNSSEC 的軟體眾多，這邊只列出現在比較多人使用且比較著名的軟體，可以確定其穩定性及功能性較符合一般需求。

也由於 DNSSEC 是基於客戶端/伺服器（Client/Server）的架構之上，所以要完整使用 DNSSEC 的話，必須伺服器以及客戶端都支援 DNSSEC。以下分伺服器端及客戶端軟體介紹。

2.3.1. 伺服器端

我們研究了目前支援架設 DNSSEC 伺服器軟體，並列出較為著名的為 BIND 及 Unbound，雖然 BIND 為目前最普及的 DNS 伺服器軟體，不過我們發現 Unbound 的設計使 DNSSEC 操作變得較簡單，因此也在此列出來做介紹。

A. BIND

BIND 是世界上最普及的 DNS 伺服器軟體，根據統計，網路上約 9 成的 DNS 伺服器是使用 BIND 所架設的。它本身是 Open Source 軟體，並且支援 Unix-like 及 Windows 平台。BIND 9.7.0 之後已經完全性的支援 DNSSEC， 包括簽署一個 Zone、動態更新、更換金鑰等功能。最新版本還簡化 DNSSEC 的設定跟 DNSSEC 的維護，更使 NSEC 的效能提升了將近 1000 倍以上。

B. Unbound

Unbound 設計成模組化的元件形式，使得它支援

DNSSEC 上變得更簡單。除此之外，模組化的優點還可以使使用者在伺服器上選擇自己想要的功能或不想要的，只要簡單的將模組裝上去或卸載，還可以自己設計自己想要的功能當成一個模組，這是跟 BIND 比起來較自由的地方。由於 Unbound 的模組化設計，使得它很快的就已加入相關模組，而具備 DNSSEC 的能力。

2.3.2. 客戶端

在客戶端方面，如果作業系統已經支援 DNSSEC，其上的應用程式不需要做任何修改，在名稱解析的過程自然會呼叫到 DNSSEC 而受到其安全保護。然而現在大部分的作業系統都沒有支援 DNSSEC，因此部份應用程式則自行實作名稱解析的部份，來支援 DNSSEC。以下介紹常見且重要的軟體支援 DNSSEC 的情況。

A. Windows 7

Windows 7 是目前唯一支援 DNSSEC 的用戶端作業系統，即使如此，其實作仍不周全。因為它僅保護了 Internet 到 Local DNSSEC 伺服器這一段的封包，封包到達 Local DNSSEC 伺服器之後，由其驗證其正確性，之後在 LAN 裡面傳遞給用戶端的過程並沒有加密，仍有被攻擊的可能性。這裡以表格的方式呈現 Windows 7 對 DNSSEC 的支援程度。

表1　Windows 7 對 DNSSEC 的支援性

	功能	敘述
支援	Establish Security Channel	在 Window 7 跟本地 DNSSEC 伺服器建立一條安全的連線
	Set DO Bit	"DNS OK"，代表客戶端已經在使用 DNSSEC

	Check AD Bit	客戶端檢查 DNSSEC 封包看是否有被伺服器驗證成功
不支援	Validator	客戶端不用透過伺服器，可以在本機做認證。
	Distinguish Security Level	使用者可以自訂不同的安全層級來滿足自己的需求

B. Firefox

Firefox 是一個相當普及的網頁瀏覽器。官方的 Firefox 尚未正式支援 DNSSEC，然而已經有一些第三方組織開始改寫 Firefox 使其支援。其中 dnssec-tools 組織（https://www.dnssec-tools.org）發表了相當多軟體的 DNSSEC 修正檔，其中也包含了 Firefox。dnssec-tools 所發表的 Firefox 修正程式，使得 Firefox 具備支援 DNSSEC 的能力，並且它是由客戶端的 Firefox 自己做驗證的，這樣的作法具備較高的安全性，不像 Windows 7 在 LAN 裡面有被攻擊的可能性。

圖1　Firefox 支援 DNSSEC

C.　Thunderbird

除了瀏覽網頁之外，收發 E-mail 也是一般客戶端最常做的事。Thunderbird 是一套被廣泛使用的 open source 收發信軟體，dnssec-tools 組織（https://www.dnssec-tools.org）也修改了 Thunderbird 使其支援 DNSSEC，同樣的它是由客戶端的 Firefox 自己做驗證的，這樣的作法具備較高的安全性，不像 Windows 7 在 LAN 裡面有被攻擊的可能性。

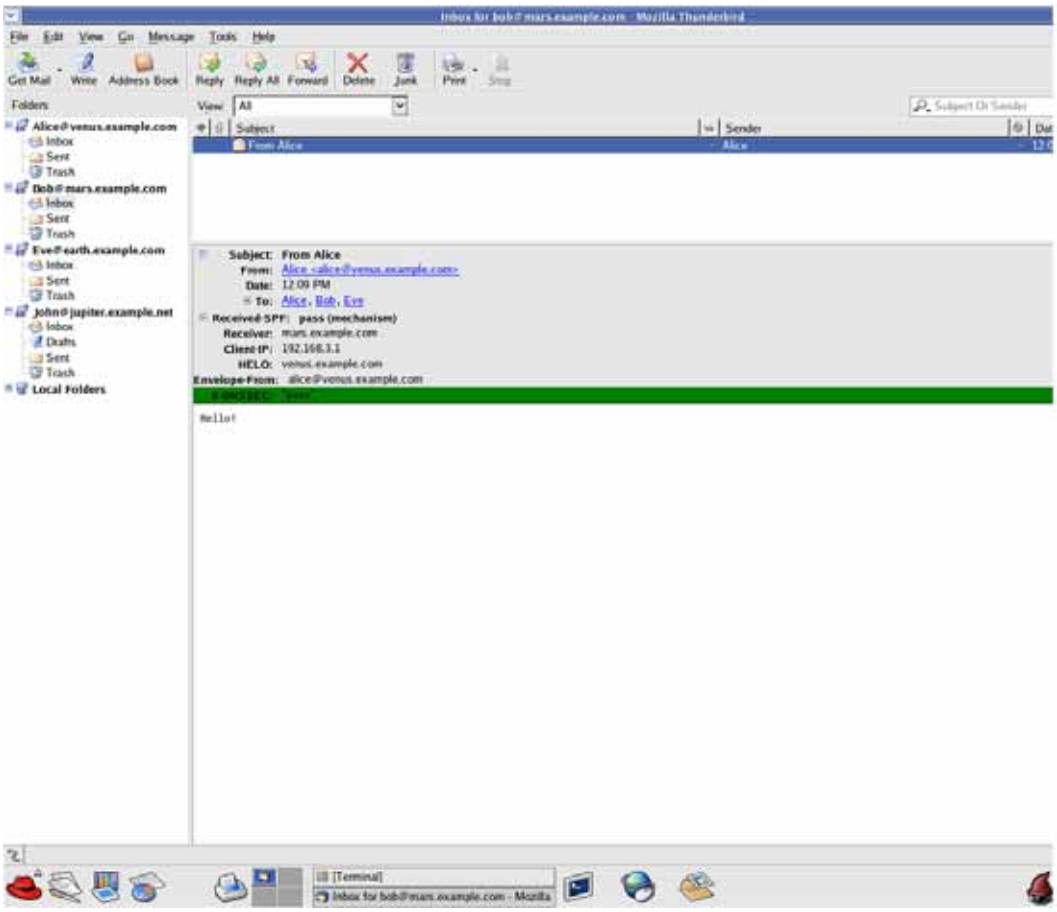

圖2　Thunderbird 支援 DNSSEC

3. DNSSEC 入門簡介

由於 DNS 沒有提供任何的安全機制，所以很容易遭到 Spoofing、Man-in-the-Middle Attack 跟 Cache Poisoning Attacks。這些攻擊都可以未來癱瘓 DNS 伺服器。基於這原因，發展出一個能使 DNS 更安全的機制顯得更加重要。

DNSSEC 最被廣泛使用的功能是「在解析網域名稱的過程中加上驗證的機制」，針對此一架構我們在我們所建置的 DNSSEC 平台上做驗證，從產生自身 DNSSEC KEY，了解如何存放 DNSSEC KEY、當有 query DNSSEC KEY 時的運作方式、及 KEY 的 revocation 做一系列的探討。

除了最初步 Key 的處理以外，最重要的功能是「在解析網域名稱的過程中加上驗證的機制」，不同網域 DNSSEC 間的認證、封包傳輸等，我們實際架設平台，並做觀測，了解 DNSSEC 間溝通方式、收到認證請求後處理認證的機制機制、如何在收到認證請求後找出相對應的 Key、最後在做回傳的動作。

在下面的圖中，清楚的說明了 DNSSEC 的 Key 及 DNSSEC 間的溝通方式，當遇到 DNS 請求時，會先回上層取得 DNSKEY 來做認證比對，確保解析網域名稱的過程是安全的，才能進行或回應下一步驟的 DNS 請求，這一系列 DNSSEC 間認證的機制看似簡單快速，但實際運作的繁瑣，不僅僅是 DNSSEC 間的溝通，更包含了 DNSSEC 上的認證機制與 DNSKEY 的存取使用。

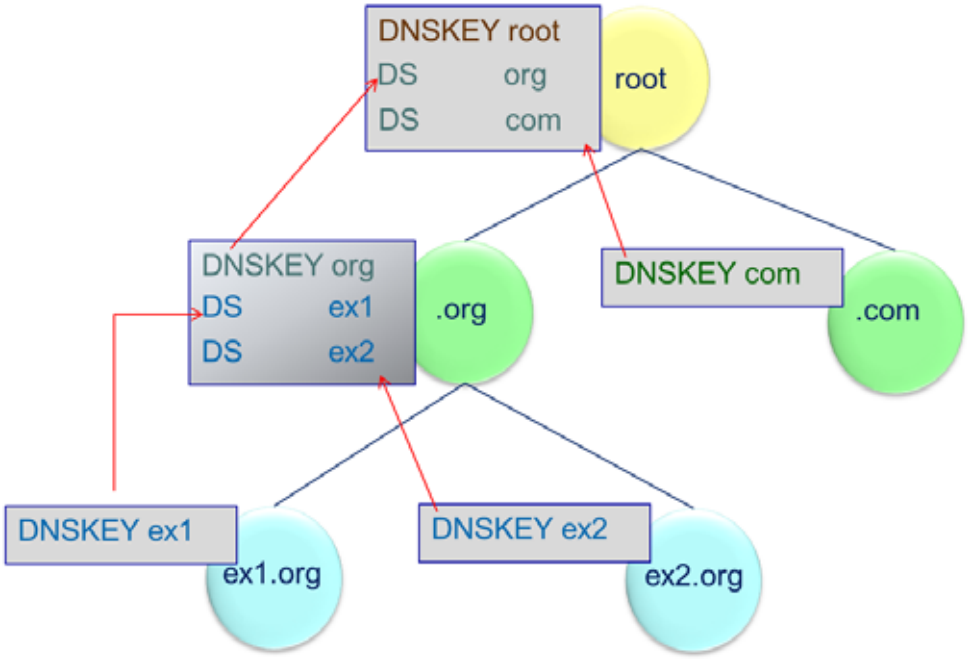

圖3 Chain of trust in DNSSEC

3.1. DNSSEC 運作概要

DNSSEC 簡單來說是在 DNS 加上數位簽章。數位簽章是基於公開金鑰架構（Public Key Infrastructure，PKI），在此架構下先產生兩把金鑰：私有金鑰（Private Key） 跟公開金鑰（Public Key），再把要加密的資料做雜湊運算（Hashing），會得到一個雜湊（Hash）值，把雜湊值用私有金鑰做加密，就會得到一串加密的字串，這串字串就是數位簽章，然後把公開金鑰公開。當客戶端取得資料時並非加密後的樣子，而是原始資料，而要驗證這個資料非偽造來源就是透過數位簽章，除了原始資料外，還會額外取得數位簽章跟來源端的公開金鑰，客戶端用公開金鑰去解開數位簽章會得到一個雜湊值，再把資料也做一次雜湊運算，也會取得一個雜湊值，再把這兩個雜湊值拿來做比對就可以知道來源是否正確。

DNSSEC 有三大保證，來源驗證性（Origin Authentication）、資料完整性（Data Integrity）、受驗證的不存在性（Authenticated Denial of Existence）。

3.1.1. 資料完整性

由於 DNSSEC 是公開金鑰架構， 公開金鑰架構的原理是：如果要保證這個資料是的完整性，我只要拿私有金鑰去簽署資料，拿到資料的人用公開金鑰去驗證，即可確定資料沒有被竄改過。所以在這個基準之下，DNSSEC 可以保證資料的完整性。

3.1.2. 來源驗證性

DNSSEC 定義了兩個新型態的資源紀錄(Resource Record，RR)去達到 Origin Authentication，DNSKEY 紀錄及 DS 紀錄。

DNSKEY 是 Zone 的公開金鑰。伺服器用私有金鑰去簽署 資源紀錄然後產生 RRSIG（Resource Record Signature），然後客戶端再用此把 DNSKEY 去驗證這個簽章。DNSSEC 伺服器會自己發佈這把 DNSKEY，如果將此把 DNSKEY 存在更高一層的 DNSSEC 伺服器則稱為 DS（Delegation Signer）。

3.1.3. 受驗證的不存在性

因為 Non-Existence 的 Replay Attack 是很嚴重的問題，因為攻擊者可以擷取了不存在的封包之後，一直對正常 DNS Request 的客戶端送不存在的訊息，導致客戶端無法拿到正確的結果。

Challenge / Response 架構是可以解決這個問題，但是要付的代價太高了，單純一個 DNS Query 就要送好多次封包。因此引進了 NSEC 的技術

3.2. DNSKEY 紀錄

在 DNSSEC 中，每個經過簽署的 Zone 都會與一對金鑰結合在一起。Zone 的私有金鑰儲存在某個安全的地方，通常放在主要 DNS 伺服器的檔案系統的檔案中。而 Zone 的公開

金鑰則會經由 DNSKEY 紀錄(這是一個 Zone 的新紀錄形態，依附在轄區的網域名稱）公諸於世。

3.3. RRSIG 紀錄

如果 DNSKEY 紀錄儲存了一個 Zone 的公開金鑰，那麼還必須有一筆新的紀錄來儲存相對應的私有金鑰的簽章，此筆紀錄就是 RRSIG 紀錄。RRSIG 紀錄會把私有金鑰的數位簽章儲存在資源記錄集（RRset）中。RRset 就是具有相同擁有者、Class 與 Type 的一群資源記錄所構成的集合；舉例來說，wormhole.movie.edu 的所有位址紀錄（Address Record）便是一組 RRset。同樣地，movie.edu 的所有 MX 紀錄是另一組 RRset。

為何是簽署整組 RRset 而不是各別的紀錄？目的在節省時間。你無法只查詢 wormhole.movie.edu 的其中一筆位址紀錄；DNS 伺服器將傳回一整組 RRset。所以當你能夠一次簽署整組的 RRset，就不用自找麻煩地一個個簽署每個紀錄了。

下面的 RRSIG 紀錄涵蓋了 wormhole.movie.edu 的所有位址紀錄：

```
wormhole.movie.edu.  3600        IN A      10.1.1.10
                     3600 RRSIG  A 5 3 3600 20100421025153 (
                                 20100322025153 40080 movie.edu.
                                 PHzzvgEcUultVA/nVY/ZvRXIDqJ4yAmcuG6k
                                 cWzXmraCtvqmU5jBXaBDI2vH/S6j0OhZygxn
                                 4NUQRqxs3uYz9YmEMKXGaklGfGPC9z2gDgIR
                                 zUMz9v/TkgTCyeKPA3t8 )
```

圖4　wormhole.movie.edu 的 RRSIG 紀錄

這筆 RRSIG 紀錄的擁有者是 wormhole.movie.edu，與所簽署之紀錄的擁有者同名。。由此可知，wormhole.movie.edu 的哪個紀錄被簽署了，就此例而言，所簽署的是 wormhole.movie.edu 的位址紀錄。所擁有的每個紀錄形態都會各有一筆 RRSIG 紀錄。

3.4. NSEC 紀錄

如果你所查詢的網域名稱並不存在於經過簽署的 Zone 中，會發生什麼事?如果 Zone 未經過簽署，DNS 伺服器只會回應"無此網域名稱"（No Such Domain Name)的回應碼。但是要如何簽署回應碼呢?如果簽署整個回應訊息，它將變得難以快取。你需要簽署某個獨特的部分，這個部分可證明你所查詢的網域名稱並不存在。

NSEC 紀錄解決了簽署負面回應訊息的問題。NSEC 紀錄用來銜接 Zone 資料中兩個前後相連之網域名稱的空隙，告訴你哪個網域名稱跟在你所指定的網域名稱後面，因此這個紀錄的名字才會叫做 Next Secure。

前後相連之網域名稱意味著 Zone 的網域名稱有一定的順序排列著，排列方式如下：首先排列網域名稱中最右邊的標籤，然後排序左邊比鄰的標籤，以此類推。標籤的排列方式為:不區分英文字母大小寫、採用字典的編排順序、數字排在字母之前、不存在的標籤排在數字之前（換句話說，movie.edu 將會排在 0.movie.edu 之前)。所以，在 movie.edu 的 Zone 中，網域名稱會被排序成這樣:

```
movie.edu
carrie.movie.edu
cujo.movie.edu
fx.movie.edu
blade.fx.movie.edu
wormhole.movie.edu
```

只有在 Zone 資料排定正是順序之後，NSEC 紀錄才有意義。底下是來自 movie.edu 的 Zone 的一筆 NSEC 紀錄，也是第一筆。

```
movie.edu. NSEC     carrie.movie.edu.    NS   SOA MX  RRSIG NSEC DNSKEY
```

這筆紀錄表示:在此 Zone 中，排在 movie.edu 之後的網域名稱是 carrie.movie.edu，也表示:網域名稱 movie.edu 擁有 NS 紀錄、SOA 紀錄、MX 紀錄、RRSIG 紀錄、NSEC 紀錄以及 DNSKEY 紀錄。

在此 Zone 中，最後一筆 NSEC 紀錄會繞回到 Zone 裡的第一筆紀錄：

```
wormhole.movie.edu. NSEC    movie.edu.          A    RRSIG   NSEC
```

這筆紀錄表示：wormhole.movie.edu 是此 Zone 的最後一個網域名稱，而排在它後面的網域名稱卻是 Zone 的第一個網域名稱，這稱為循環邏輯（Circular Logic）。

如果你在內部查詢 www.movie.edu，你將取得 wormhole.movie.edu 的 NSEC 紀錄，告訴你 www.movie.edu 並不存在，因為在此 Zone 中，wormhole.movie.edu 之後已經沒有紀錄了。

NSEC 紀錄相當重要，它可以明確區分哪些資料不存在於 Zone 中。可以防止攻擊者謊稱實際上存在的網域名稱或紀錄不存在的攻擊。

但是 NSEC 還是有一定的風險存在，攻擊者可以查詢你 Zone 的網域名稱所依附的 NSEC 紀錄，找到以字典編排順序排列的下一筆網域資料，然後重複此程序已得知 Zone 中所有的網域名稱。

3.5. DS 紀錄與信任鍊（Chain of Trust）

到目前為止，在我們簽署過的 Zone 裡，每組 RRset 都會被關聯到一筆 RRSIG 紀錄。為了讓其他人能夠驗證這些 RRSIG 紀錄，我們的 Zone 會以 DNSKEY 紀錄像全世界公佈其公開金鑰。但假設有人侵入了我們的主要 DNS 伺服器。根本無法阻止它產生自己的金鑰對（Key Pair)。然後他會竄改

我們的 Zone 資料，以他剛產生的私有金鑰重新簽署我們的 Zone，並以 DNSKEY 對外公布他剛產生的公開金鑰。

為了防治此問題，我們的公開金鑰必須經過較高管理當局的認證。舉例來說，較高管理當局須證實我們在 DNSKEY 紀錄所公佈的 movie.edu 公開金鑰，確實屬於管理 Zone 的組織所有，而非來自有心人士。在認證我們之前，較高管理當局需要我們證明自己的身分以及我們確實是管理 movie.edu 的責權單位。

這個較高管理當局就是我們的上層 Zone: edu。當我們產生自己的金鑰對以及簽署了 Zone 之後，我們還得將自己的公開金鑰傳送給 edu 的管理者，並隨附資料證實自己的身分以及我們是 movie.edu 的責權單位。他們會透過將 DS 紀錄插入 edu 之 Zone 的方式指出認可我們的憑證以及我們的公開金鑰，然後會使用他們的私有金鑰簽署該紀錄。

DS 的全名為 Delegation Signer。DS 紀錄用於指認經授權可簽署 movie.edu 的 Zone 資料的公開金鑰。伴隨著 DS 紀錄的是一筆 RRSIG 紀錄，用來表示 edu 之 Zone 的管理者簽署了 movie.edu 的 DS 紀錄，因此可以保證它的真實性。

當根據 edu 的 DNS 伺服器的指引資訊前往 movie.edu 伺服器以及驗證 movie.edu 之 DNSKEY 紀錄的時候，你的 DNS 伺服器首先會驗證涵蓋該 DS 紀錄的 RRSIG 紀錄。假定該 RRSIG 紀錄通過驗證，則你的 DNS 伺服器會查詢依附在 movie.edu 的所有 DNSKEY 紀錄，並從中找出與 DS 紀錄所列示的 Key Tag 和演算法欄位值相符的 DNSKEY 紀錄。一旦找到正確的 DNSKEY 紀錄，你的 DNS 伺服器透過單向雜湊運算（One-Way Hash）演算法檢視該紀錄，檢查其 Digest 是否相符於 DS 紀錄的 Digest。如果相符，DNSKEY 紀錄就是可信賴的，而你的 DNS 伺服器可以用它來驗證涵蓋 DNSKEY、 RRset 的 RRSIG 紀錄或著是被相對應的私有金

鑰簽署過的其他 RRsets。

如果有人侵入了 edu 之 Zone 的主要 DNS 伺服器，因為 edu 之 Zone 的 DNSKEY 紀錄經 Root Zone 的一筆 DS 紀錄認證過，所以他們無法輕易換掉它，或是用它來簽署任何資料。Root Zone 的公開金鑰廣為人知，而且被設定在每部支援 DNSSEC 的 DNS 伺服器上。

4. DNSSEC 與憑證相關技術研究

DNSSEC 最被廣泛使用的功能是「在解析網域名稱的過程中加上驗證的機制」，除此之外，它還能夠用來擺放憑證。

近年來憑證使用的情況為，公開金鑰基礎設施（Public Key Infrastructure，PKI）藉著憑證管理中心（Certificate Authority ，CA）將使用者的個人身分跟公開金鑰鏈結在一起，成為一個使用者憑證，因普遍是商業經營，申請憑證的價錢對於普通大眾來說太昂貴，導致憑證並未被廣泛使用。若如今有公開可信任的機構（例如：學校、公司行號…等）欲自行簽發免費憑證，社會上也能相信此機構擔保下的憑證，讓人們願意去申請，則憑證的普及率能更加提升。

由於 DNSSEC 伺服器之間資料傳遞時，會加以驗證來源與訊息內容之可信度，確保真實性與完整性。DNS 伺服器早已遍布地球，要改設成 DNSSEC 系統完全不需要額外的硬體設備。綜合以上優點，各單位將簽發的憑證放置於 DNSSEC 伺服器中是非常恰當的，只要有網路即可查詢的到，無地域限制，使得憑證易於取得而能夠全球性的被使用，即可在不影響現有網路架構為考量，無負擔的達成 Global PKI 的理想。若大量網路應用都能結合 Global PKI 的機制，讓安全層級多一道保障，就能大幅提升整個 TCP/IP 網路的安全性。以下將會以三個現有網路應用為主軸，個別分析其使用現況與問題。接著闡述這些應用與 global PKI 結合後，如何解決其問題之可行運作方式與好處做詳盡的說明。

4.1. Secure E-mail

近年來，E-mail 已成為人們聯繫關係的主要溝通管道之一，諸如社交圈、就職公司…個人隱私都能藉由窺探 E-mail 信箱知悉，其安全性的重要無庸置疑。但 Secure E-mail 的應用軟體早已在網路上流通多年，為什麼仍未被廣泛使用呢?因

為未有 Global PKI，人們運用憑證不便。當使用者要寄加密郵件前，必須先取得收件者的憑證，並取出憑證中的公鑰加密郵件。而收件者也必須從寄件人的憑證內取得公鑰才能驗證數位簽章。若今使用者要寄重要訊息給公家機關、或是欲洽談合作之商業人士時，可能因未能輕易取得收件者憑證造成無法順利寄件。實際上，DNSSEC 與 Secure E-mail 的架構結合是無所衝突卻很合適。下面針對 Secure E-mail 最廣為人知的兩套系統 S/MIME 與 OpenPGP 做更詳盡的分析。

4.1.1. S/MIME

S/MIME (Secure/Multipurpose Internet Mail Extensions) ，一種 Internet 標準，遵循 X.509 之憑證使用協定，管理欲加密的電子郵件如何發送和接收。目前 S/MIME 實作搭配憑證管理中心發佈憑證與 LDAP 查詢憑證，並且使用者需額外付費給憑證管理中心與 LDAP。當使用者要驗證憑證時，必須事先得到大家公認最高等級之憑證管理中心的憑證（Root Certificate），才能一層層的擔保下游的憑證管理中心，還要先知道 LDAP 伺服器的位址才能查詢，流程繁複。若能搭配 DNSSEC 實作將會有更簡單、好用的架構。

RFC 4398 內容中，提及在 DNSSEC 伺服器上放置與查詢憑證的方式。舉例說明，當使用者欲查詢“receiver@office.com”的憑證資訊，我們會先將它轉換成“receiver.office.com”的 Domain Name 表示格式，接著在 DNSSEC 伺服器中查詢。由於 DNSSEC 的階層性架構中，已含有分層驗證的機制，再加上只需將 E-mail 轉換格式，即可依 DNS 規則連線到 DNSSEC 伺服器查詢憑證。

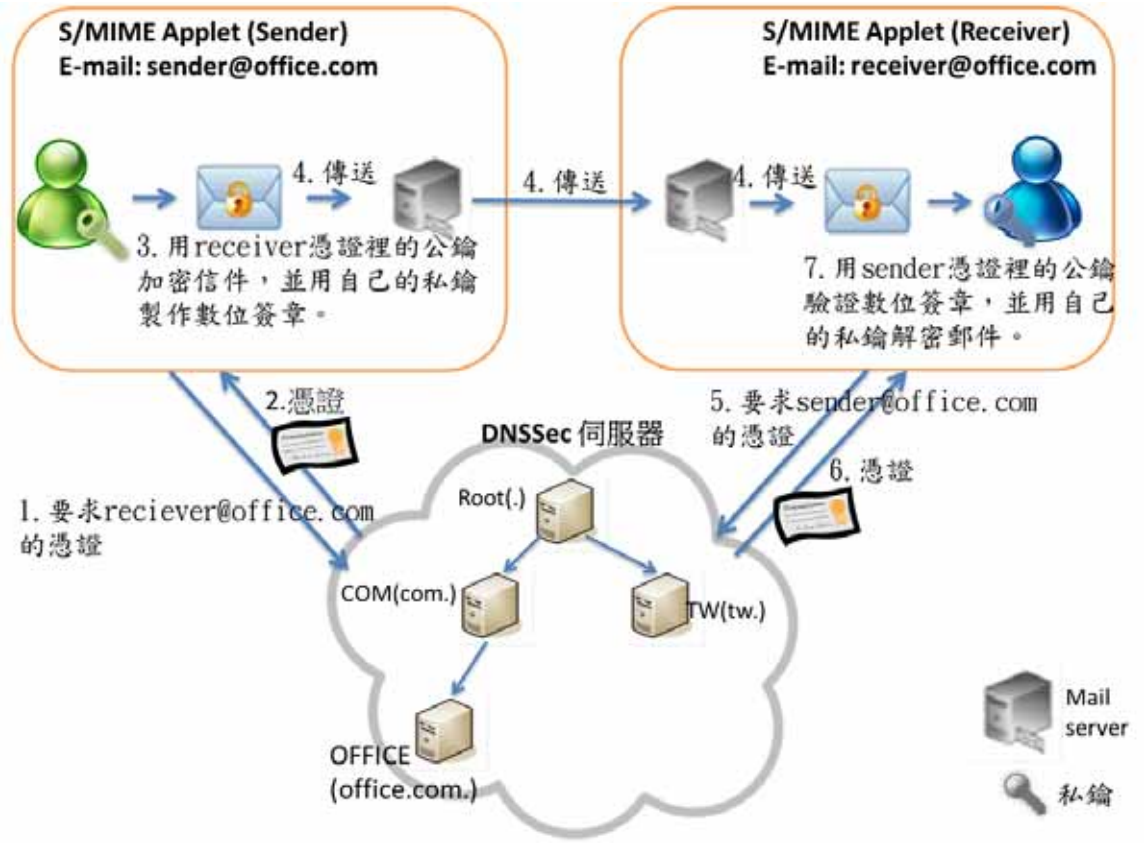

圖5　DNSSEC 架構與 S/MIME 結合後的運作流程圖

4.1.2. OpenPGP

同樣也是電子郵件加密系統，與 S/MIME 不同的是 OpenPGP 系統使用自行發佈的憑證，並搭配“Web of Trust”的方式，讓已被信任的第三方對此新申請的憑證背書，保證此憑證是有效可用的。讓用戶間自行建立信任網，並沒有共同的信任中心做保證。雖不用另外付費給憑證認證中心與 LDAP，但使用上較缺乏安全性上的保障。如果當一個新的憑證產生時，未能找到第三方來背書，則此憑證就無所用武之地了。

若 OpenPGP 系統結合 DNSSEC，將自行產生的憑證都放到 DNSSEC 伺服器上。因為 DNSSEC 伺服器的內容是可公開被查詢的，再加上 DNSSEC 伺服器管理者只允許經過認可的 OpenPGP 能夠放置憑證，則所有的用戶只要能在 DNSSEC 伺服器找到 OpenPGP 的憑證，必

定是真確可信任的，且不須另外請第三方背書。

4.2. IP Security（IPSec）

IPSec 是針對位於網路層的 Internet Protocol 所提出的安全性協定。利用非對稱式加密法來建立安全連線，接著使用對稱式加密法來加密傳輸的資料。IPSec 為了便於建立與管理加密時所需各類金鑰，預設採用 Oakley 為金鑰交換協定。Oakley 的原理與 Diffie-Hellman 金鑰交換法相似，但能提供較高的安全性。通訊的雙方必須先交換各自的公鑰，再依對方的公鑰與自己的私鑰算出共同的密鑰。公鑰交換最常見的情況有兩種：無條件信任微軟，然後相信微軟信任的 CA。所以使用微軟放置於電腦內的 Root CA 資訊，驗證對方的憑證；第一次通訊時，無論對方傳來的憑證是否經合法 CA 擔保都姑且相信，有安全上的風險。如果 IPSec 用戶端，可經由查詢 DNSSEC 伺服器得到通訊對方憑證中的公鑰，即可解決以上問題，讓 IPSec 更可靠的運用於網際網路。在下一段舉例說明。

網路上的使用端 A、B，A 端想和 B 端（IP：168.110.32.56）通訊，要先取得 B 端的公鑰。欲查詢 IP：168.110.32.56 的憑證，如同 DNS 反查機制，將 IP 的四組數字反著擺，然後附加 in-addr.arpa 網域（負責接受反查服務之網域）到反向位址的末端，變成“56.32.110.168.in-addr.arpa”，就能夠依照此順序在 DNSSEC 伺服器中查詢到對應 IP 的憑證中之公鑰。B 端也能如法炮製取得 A 端之公鑰，進而建立 A、B 端之間的安全連線。

4.3. Transport Layer Security（TLS）

TLS 保證傳輸層通訊間的保密性和可靠性。利用公鑰基

礎設施為核心技術，將網路連線加密，對端點身份認證與通訊保密，提供網路通訊安全性及數據完整性的一種協議。不過實際運作時，大部份的情況只有網路服務端單方面被進行身份驗證，至於客戶端因為並非全面持有憑證，而未能確實驗證身份。假設此網路服務端是一個購物網站，在無法依據憑證驗證客戶端身份、又沒有設置其他的安全機制的情況下同意交易，有可能因客戶端的被盜會員帳號、身份被假冒，造成網路交易糾紛。如果網路上已全面佈建 DNSSEC 伺服器，人人皆踴躍申請可靠且免費的憑證，達成 Global PKI 的構想，此問題即可迎刃而解。TLS 就能確實完成對端點身份認證的機制，營造一個安全的網路平台。

4.4. 結論

將憑證放置於 DNSSEC 伺服器上發展 Global PKI，對於現有網路架構上改變的範圍很小，但帶來的衝擊卻很大。對於發佈憑證的機構，若肯用心維護管理憑證的環境，必定可增加人們對此機構之信用度，而且申請的人越多，使用越廣泛，無疑是對此機構的免費宣傳；對於憑證用戶端，不一定要向憑證管理中心申請昂貴的憑證，即可在使用網際網路時大幅增加安全性的保護；對於網路服務端，省去管理帳號密碼的心力，使用更安全有保障的憑證認證機制。Global PKI 能初步過濾訊息來源，增加網路應用的可靠性。觀念如同電話來電顯示，若顯示號碼保密則需對來電者多一份警惕。可應用於電子郵件、廣告、網站、軟體下載…等等。Global PKI 能依個人、學校機關、公司行號、職業、城鎮、國家等不同的對象設計出各種類型的憑證，使憑證運用上更加彈性。

推廣 Global PKI 是必須且指日可待的，不管是什麼應用，縱使已聲名遠播，都必須不斷增加其安全性，才能長久發展，例如：Facebook 經常性的更新改進。而達成 Global PKI 後，世界的改變更令人期待。

5. DNSSEC 與 IPv6 相關技術研究

目前網際網路普遍使用的 IPv4 網路協定，其所能提供的網路位址已面臨嚴重不足的窘境，IPv6 為新一代的 IP 標準，推廣了多年雖然普及率還不算高，但由於其擁有大量 IP 等優勢，仍被看好為未來取代 IPv4 的重要標準，目前大部分的網路基礎建設也都支援 IPv6，並且在 2004 年 7 月，「網際網路網域名稱與位域管理機構（ICANN）」宣佈根網域的 DNS 伺服器開始支援 IPv6。而 DNSSEC 作為 DNS 的延伸性安全標準，如果不能完全支援 IPv6，對長期的發展將相當不利。

5.1. IPv6 簡介

IPv6（Internet Protocol version 6，IPv6）的誕生是由於 1981 年制定的 IPv4（Internet Protocol version 4，IPv4）的 IP 位址快速消耗，使得 IP 位址短缺的問題快速浮現，日本 Surfpoint 網路統計機構甚至預估現行的 IPv4 位址即將於 2016 年用罄。於是網際網路專案任務小組（Internet Engineering Task Force，IETF）在 1998 年 12 月正式提出 IPv6，其標準規範定義在 RFC 2460 中。

IPv4 用 32 位元長度來表示位址，分成 4 組 8 位元的欄位，為了讓人容易閱讀跟記憶，通常採十進位表示法，例如 140.113.1.1。每個欄位的範圍從 0 到 255，可以提供 2^{32}（4,294,967,296)個可用位址，但其中有部分被保留做為特殊用途，例如 127.x.x.x 給本機位址使用、224.x.x.x 為多播位址段、255.255.255.255 為通用的廣播位址、10.x.x.x，172.16.x.x 和 192.168.x.x 給私有網路使用。所以實際可以使用的 IP 位址不到 2^{32}（4,294,967,296)個。

IPv6 用 128 位元長度來表示，位址位址空間可達 2^{128}—大約 3.4x1038 個位址，分成 8 組 16 位元的欄位，採用十六

進位表示法，每個欄位的範圍從 0000 到 ffff，例如

0234:5678:abcd:0000:0000:0000:beef:0678

5.2. IPv6 位址表示

各個欄位中的十六進位數字介於0-9或A-F(不分大小寫)，在此也可以歸納出幾點規則:

每個欄位的 32 位元的開頭 4 位元為 0，可省略 0 不寫

每個欄位的 32 位元都是 0，可簡寫成 0

如果有連續欄位的 32 位元都是 0000，可省略只寫兩個冒號"::"，但一個位址中只能用一次

依照這規則剛的例子可簡化為：

234:5678:abcd::beef:678

如果要在位址後面加上 port number 的話，就會用中括號將 IPv6 的位址包起來，避免原本的冒號跟接在後面的冒號混淆。例如:

[234:5678:abcd::beef:678]:21

5.3. IPv6 的特色

- 大量位址空間

IPv6 通訊協定採用 128 位元長度的位址空間，可抒解 IPv4 位址不足對於各式網路應用造成的限制，而 ISP 業者也可因省去網路位址解析設備（Network Address Translation，NAT）或 IP 分享器等設備而降低營運成本，並減少網路上的瓶頸。

- 位址自動配置

IPv6 通訊協定支援自動組態（auto-configuration），

因此 IPv6 主機接上 IPv6 網路後可自動取得 IPv6 網路位址資訊，無須如 IPv4 網路另外獨立設置 DHCP 伺服器。這種「隨插即用」的特色可以減輕網路管理者及使用者發放與設定 IP 位址的負擔。

- 網路層安全性

IPv6 通訊協定內建 IPSec 加密機制，透過延伸表頭表示封包本身是加密或經過認證簽署的，因而大幅提昇網路安全性。

- 行動性（Mobility）

Mobile IPv6 可提供較 Mobile IPv4 更強大的移動性，解決以往跨網段漫游所發生的連線障礙。

- QoS 機制強化：

IPv6 協定透過封包中基本表頭內的優先順序欄位及流程控制標記等欄位，可直接支援 QoS 機制。此特性對於講求即時性的多媒體傳輸應用而極有助益

5.4. IPv6 與 DNS

在 DNS 上，IPv6 的正向解析是使用 AAAA 紀錄，反向解析在 ip6.arpa（原先 ip6.int）下進行，而 RFC 3363 中對 AAAA 模式給與了有效的標準化。舉例來說在 DNS 伺服器上設定如下：

```
www.example.com        AAAA        234:5678:abcd::beef:678
www.example.com    A            123.123.123.123
```

即表示 www.example.com 的 IPv6 位置為 2001:0DB8::1428:57ab，IPv4 地址為 123.123.123.123，一台主機也能同時擁有 IPv6 和 IPv4 的地址而不衝突。

```
02345678abcd000000000000beef0678.ip6.arpa.      IN   PTR
www.example.com.
```

表示 www.example.com 的反向解析。

5.5. IPv6 與 DNSSEC

由於佈署 IPv6 不太可能很快得全面都更新成 IPv6 的環境，一定會有 IPv4 跟 IPv6 共存的情況，因此我們要確保在這個環境下 DNSSEC 伺服器還是可以正常的運作。

我們做了以下的實驗 ：

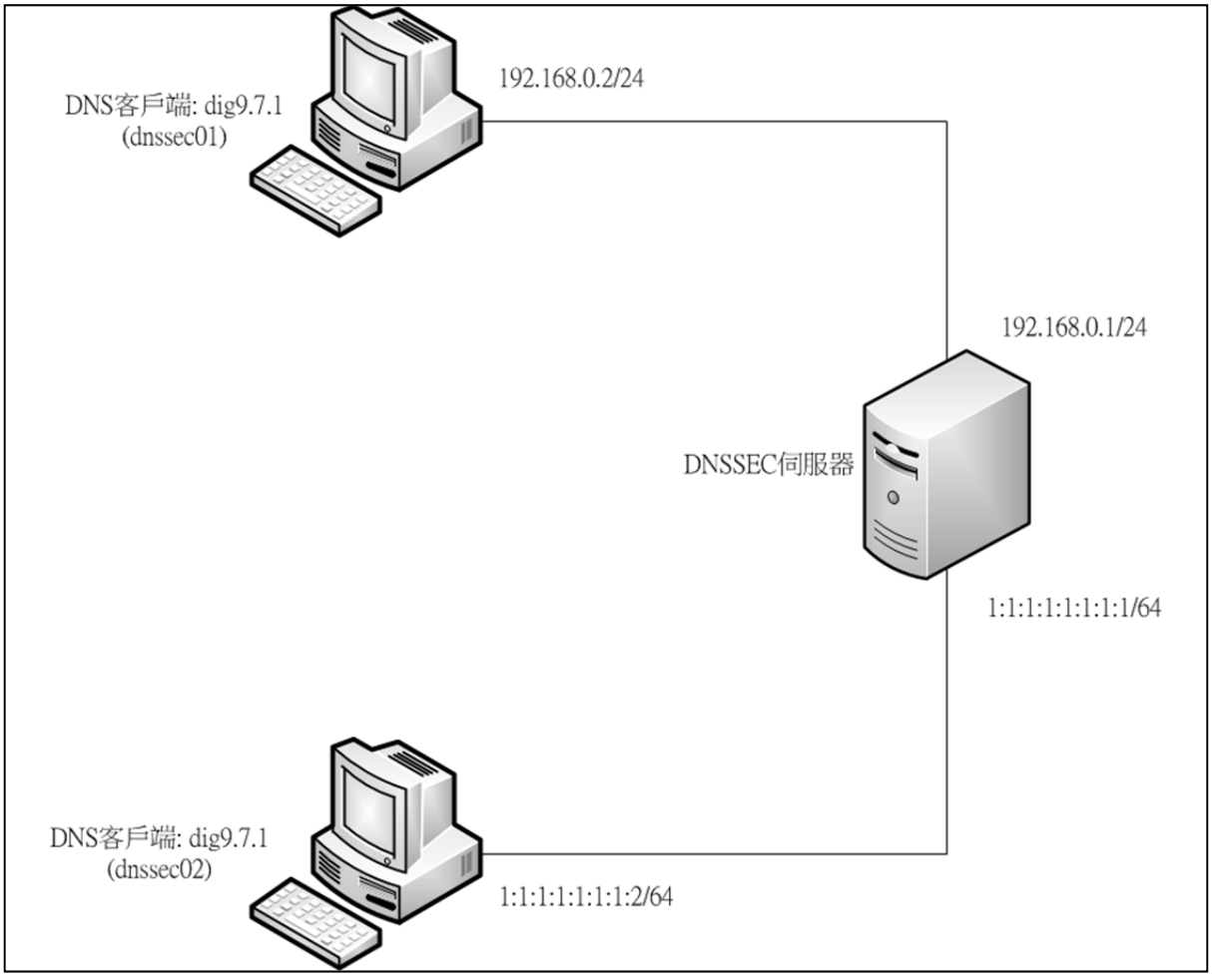

圖6　IPv6 對於 DNSSEC 相容性實驗環境

利用有兩台分別是 IPv4 及 IPv6 環境的客戶端及一台有兩張網路卡可以同時處理 IPv6 及 IPv4 封包的 DNSSEC 伺服器。其中，IPv6 客戶端的 IP 為 1 :1 :1 :1 :1 :1 :1 :2/64，而 IPv4 客戶端的 IP 為 192.168.0.2/24，我們利用這兩台 IPv4

及 IPv6 客戶端分別對 DNSSEC 伺服器分別送出 DNS 請求，發現伺服器端傳回的結果皆是正確的，回應結果如下，也證明了 DNSSEC 針對來自 IPv6 及 IPv4 請求可做出無誤地回應，因此經由這次實驗也可以保證 DNSSEC 對以後即將來臨的 IPv6 是完全性支援的。

```
root@dnssec01:/home/dnssec01# dig +dnssec www.example.com

; <<>> DiG 9.7.1-P2 <<>> @1:1:1:1:1:1:1:1 www.example.com
; （1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26326
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.example.com.          IN   A

;; ANSWER SECTION:
www.example.com.    38400   IN   A         192.168.0.4
www.example.com.    38400   IN   A         192.168.0.2
www.example.com.    38400   IN   AAAA      1234:1234::ff
www.example.com.    38400   IN   RRSIG     A 5 3 3600 20101221135501 2010122135501 6477 example.com. aIOT7U/CRcFi3CcgaHp6EqV8JHkODodQM0Pg7CKh1gby4/8pGnqABDiU

;; Query time: 5 msec
;; SERVER: 1:1:1:1:1:1:1:1#53（1:1:1:1:1:1:1:1)
;; WHEN: Wed Dec 28 14:15:52 2010
;; MSG SIZE  rcvd: 152
```

```
root@dnssec02:/home/dnssec02# dig +dnssec
```

```
www.example.com

; <<>> DiG 9.7.1-P2 <<>> @192.168.0.1 www.example.com
; （1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47441
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0,
ADDITIONAL: 0

;; QUESTION SECTION:
;www.example.com.          IN    A

;; ANSWER SECTION:
www.example.com.    38400    IN    A          192.168.0.4
www.example.com.    38400    IN    A          192.168.0.2
www.example.com.    38400    IN    AAAA       1234:1234::ff
www.example.com.    38400    IN    RRSIG      A    5    3    3600
20101221135501      2010122135501      6477      example.com.
aIOT7U/CRcFi3CcgaHp6EqV8JHkODodQM0Pg7CKh1gby4/8pGnqA
BDiU

;; Query time: 4 msec
;; SERVER: 192.168.0.1#53（192.168.0.1)
;; WHEN: Wed Dec 22 01:02:09 2010
;; MSG SIZE    rcvd: 152
```

5.6. 結論

IPv6 為新一代的 IP 標準，推廣了多年雖然普及率還不算高，但由於其擁有大量 IP 等優勢，仍被看好為未來取代 IPv4 的重要標準，目前大部分的網路基礎建設也都支援 IPv6，並且在 2004 年 7 月，「網際網路網域名稱與位域管理機構（ICANN）」宣佈根網域的 DNS 伺服器開始支援 IPv6。由此

實驗結果可以得知，DNSSEC 對以後即將來臨的 IPv6 是完全性支援的。

6. DNSSEC 與中文網域名稱相關技術研究

IETF 於 2003 年 3 月發布通過國際化域名（IDN)技術標準有關之 3 篇 RFC 之後，在網域名稱上使用非拉丁字母已經變得可能，根據相關標準，中文網址可透過轉換為中介 Punycode 的方式，在網路上變得通用。而在 2009 年 10 月 30 日，「網際網路網域名稱與位域管理機構（ICANN）」開會通過，開放網域名稱直接使用非拉丁字母，也就是可不再透過 Punycode 轉譯，初期僅佈署到國際頂級域名（TLDs），後續的實作與佈署預期也將逐漸普及。目前來說，中文網址的普及率雖不算很高，然而仍是國際標準的一部分，並且有一定數量的使用者，DNSSEC 作為 DNS 的延伸性安全標準，同樣必須考慮到升級到 DNSSEC 之後的相容性問題，確保中文網域名稱能正確使用。

6.1. 國際化域名（IDN)

國際化域名(Internationalized Domain names, 簡稱 IDNs)採用 Unicode 以支援不同國家的域名，不過這種作法會使得整個 DNS 的架構需要作一些修改以配合 Unicode 的使用。為了能在原有的 DNS 架構上，且不會對 DNS 架構做修改的前提之下，在 2003 年五月由 P. Faltstrom, Cisco、P. Hoffman, IMC & VPNC、A. Costello, UC Berkeley 三個人訂出了 Internationalizing Domain Names in Applications 簡稱（IDNA)，RFC 3490。IDNA 訂出了以原有的 ASCII 搭配一些特別字元表示非 ASCII 的方式，讓 DNS 可以容易的支援各國語言的網域名。IDNA 允許 DNS 利用特殊字元（指非 26 個英文字母)作為字首搭配 ASCII，組合以代表一個非 ASCII 的網域名稱。這種作法可以使底層的協定及上層的應用程式（DNS Server, Resolver)完全不需要特別處理這些非 ASCII 字元所構成的網域名稱，在不改變現有 DNS 架構下, 使用者也能透過非 ASCII 構成的域名連到正確的網站。

IDNA 描述了可以透過 ASCII 字元來表示 Unicode 及其它非 ASCII 的字元，而在實際上另外有 RFC 3492（Punycode: A Bootstring encoding of Unicode for Internationalized Domain Names in Applications ）描述了如何以 ASCII 表示其它非 ASCII 的字元。而 Punycode 本身就是 ASCII，為了讓 Punycode 足以表達所有的非 ASCII 字元，Punycode 需要具有以下的特性：Completeness、Uniqueness、Reversibility、Efficient encoding、Simplicity、Readability。

- Completeness

  可以用基本的字元組合表達所有 Unicode 的字串。

- Uniqueness

  一個 unicode 的字串只能對應一組的 punycode。

- Reversibility

  所有 punycode 對應的 unicode 字串，皆可回推成 ASCII 字元的組合。

- Efficient encoding

  對應一組 unicode 字元，產生出的 punycode 長度必須有所限制。

- Simplicity

  產生 punycode 的演算法及反推的演算法都要容易實作。

- Readability

  產生出的 punycode 及來源字串相似度要接近。

6.2. 異體中文域名

異體中文域名，指的是繁體中文與簡體中文。因為 Unicode 並沒有建立繁體字與簡體字的對照關係，導致一個相

同意義的中文網域可能同時代表多個網域名稱。例如：臺灣、台湾。如果有惡意人士申請了“臺湾”，便能夠輕易的做到 IDN homograph attack。

為了解決此一問題，目前在申請中文域名時，已明令禁止申請繁簡夾雜的網域名稱，並且在申請時一個中文域名所對應簡體對照字組合域名及相關組合域名將被視為同一套中文域名，未來無法再另外申請簡體的中文域名。例：“台網中心”之簡體對照字組合域名為“台网中心”。

相關的 RFC 有兩篇：

1) RFC 3743（Joint Engineering Team （JET) Guidelines for Internationalized Domain Names（IDN) Registration and Administration for Chinese, Japanese, and Korean）（Informational, 2004)

2) RFC 4713（Registration and Administration Recommendations for Chinese Domain Names）（Informational, 2006)

由於 IDN 標準是技術協定方面的標準，並未包括中文異體字的需求，為避免引起異體中文域名間註冊之混淆及爭議，RFC 3743 定義了異體字表的 Valid Code Point、Preferred Variant、Character Variant 三個欄位，以及異體字表應用在 IDN 域名註冊管理之處理原則。

因為 RFC 3743 定義的是一般性的基礎原則， CDNC 成員之 TWNIC 與 CNNIC 在 RFC 3743 的基礎下，針對中文域名的異體字對應的需求，共同研擬了 RFC 4713，提出在 RFC 3743 定義之異體字表結構下如何處理中文域名之原則，以及將 RFC 3743 中之 optional process 作進一步的說明。

6.3. IDN 標準帶來的影響與對應解決方法

現今 IDN 的支援，除了少部分 Top-level Domain 不須透過 Punycode，在大部分的網域仍然是透過 Punycode 來轉譯非 ASCII 的字元。以下將以實例說明如何透過簡單的設定，不用改變原有的架構下，能夠使用中文網址連到正確對應的網站。這些設定有三個方面，分別是 DNS 伺服器、WEB 伺服器、以及瀏覽器。

1) 在 DNS 伺服器方面，只要對 zone file 作修改，將網域轉成 Punycode 即可。這裡要注意的是，在 zone file 內除了繁體的 Punycode、簡體的 Punycode 同樣也要在設定一次。

```
zone "台灣.tw" {
type master;
file "taiwan.tw";
};
```

圖7　原 named.conf 部分設定

```
zone "xn--kpry57d.tw" {
type master;
file "taiwan.tw";
};
```

圖8　轉換後之 named.conf 部分設定

```
;
$TTL 86400
;
@ IN SOA dns.taiwan.tw.(
20030420 ; Serial
36000 ; Refresh
7200 ; Retry
3600000 ; Expire
86400 ); Minimum
IN NS dns.taiwan.tw.
;
台北 IN A  127.0.0.1
新竹 IN NS dns2.taiwan.tw
```

圖9　原 zone file 設定

```
;
$TTL 86400
;
@ IN SOA dns.taiwan.tw.(
20030420 ; Serial
36000 ; Refresh
7200 ; Retry
3600000 ; Expire
86400 ); Minimum
IN NS dns.taiwan.tw.
;
xn--djrpt   IN A  127.0.0.1
xn--efvt78b IN NS dns2.taiwan.tw
```

圖10 轉換後之 zone file 設定

2) 在 Web 伺服器方面，同樣也只要將 Virtual host Name 及主機名稱換成 Punycode 即可。

3) 在瀏覽器上，使用者在輸入中文網域名稱之後，瀏覽器將會自動的把中文網域名稱轉換成 Punycode，再以此 Punycode 向 DNS 伺服器查詢。IE6.0 與更早的

版本都無法支援中文網域名稱，使用者必須先行安裝另外的外掛程式，先將中文域名另外解析後再傳回瀏覽器,相關軟體有:TWNIC 所釋出的“中文通”軟體。而目前 IE7 以後的版本與 Safari、Chrome、Firefox 都能完整的支援中文域名。

6.4. Internationalized country code top-level domain

為了完全符合 IDNs 的規範，最終仍須重新建置 DNS，使得網域名稱可以採用 Unicode 而不再需要透過 Punycode 的轉碼，但一直到了今年才開始在 Top-level 的 Domain 上建置，未來將逐漸普及。

2010 年 5 月 5 日建置了第一個 Internationalized country code top-level domain 使得阿拉伯語系的國家可以不再透過 Punycode 轉譯而直接解析阿拉伯文構成的網域名稱。

一個 Internationalized country code top-level domain（簡稱 IDN ccTLD）負責 DNS 的網路架構中最上層的 Domain，而負責這個 Domain 的伺服器可以不透過 Punycode 的轉碼，使用當地的語言就可以解析在該網域下的網域名稱。

2010 年 6 月 25 日”.台灣” 與 “.中国” 與 “.香港” 申請成為 ccTLD。雖然重新建置 DNS 已經逐漸開始，但完整的網域解析仍然要靠下層的 DNS，逐一解析才能正確使用中文網域名稱，所以解析中文網域名稱目前為止，依然需要依靠 Punycode 的轉碼才能使用中文網域名稱。

6.5. DNSSEC 與中文域名相容性

因為目前大部分中文網域之解析主要還是依靠 Punycode 的轉碼，而 Punycode 又是以 ASCII 來表示的，所以 DNS 不須更動架構，而新增一個 Domain name 紀錄與以前並無不同,新增一個中文域名就和新增一個英文域名相同，

經 Punycode 轉碼後的中文域名其構成的字元與英文域名同樣都是 ASCII，而且經過實際的測試可以確定非 Top-level domain Name 中文域名與 DNSSEC 的相容性是沒有問題的。

6.6. 結論

因為目前大部分中文網域之解析主要還是依靠 Punycode 的轉碼，而 Punycode 又是以 ASCII 所構成的，所以不須更動 DNS 的架構，新增一個 Domain Name 紀錄與以前並無不同。更明白地說，新增一個中文域名就和新增一個英文域名完全相同，經 Punycode 轉碼後的中文域名其構成的字元與英文域名同樣都是 ASCII。對於 DNSSEC 來說，DNSSEC 會對 Zone File 進行簽章的動作，如果 DNSSEC 可以無誤地對英文網域名稱的 Zone File 簽章，那我們可以推斷經過 Punycode 轉碼的中文網域名稱 Zone File 也能被正確地簽章。在實際上，經過完整的測試可以確定非 Top-level domain Name 中文域名與 DNSSEC 的相容性是沒有問題的。

7. DNSSEC 網路測試實驗室建置

為了執行本計畫所需的實驗，我們建置了一個 DNSSEC 實驗室。在這個實驗室中，我們做了一個三層網域的架構，如下圖所示，每一個網域採用兩台 DNSSEC 伺服器做 master/slave 的架構，同時額外使用一台伺服器擔任 CA 的角色，用以發行憑證。伺服器間的溝通使用 Gigabit Ethernet 來提供超高速網路頻寬，並且所有設備都能夠支援 IPv6。

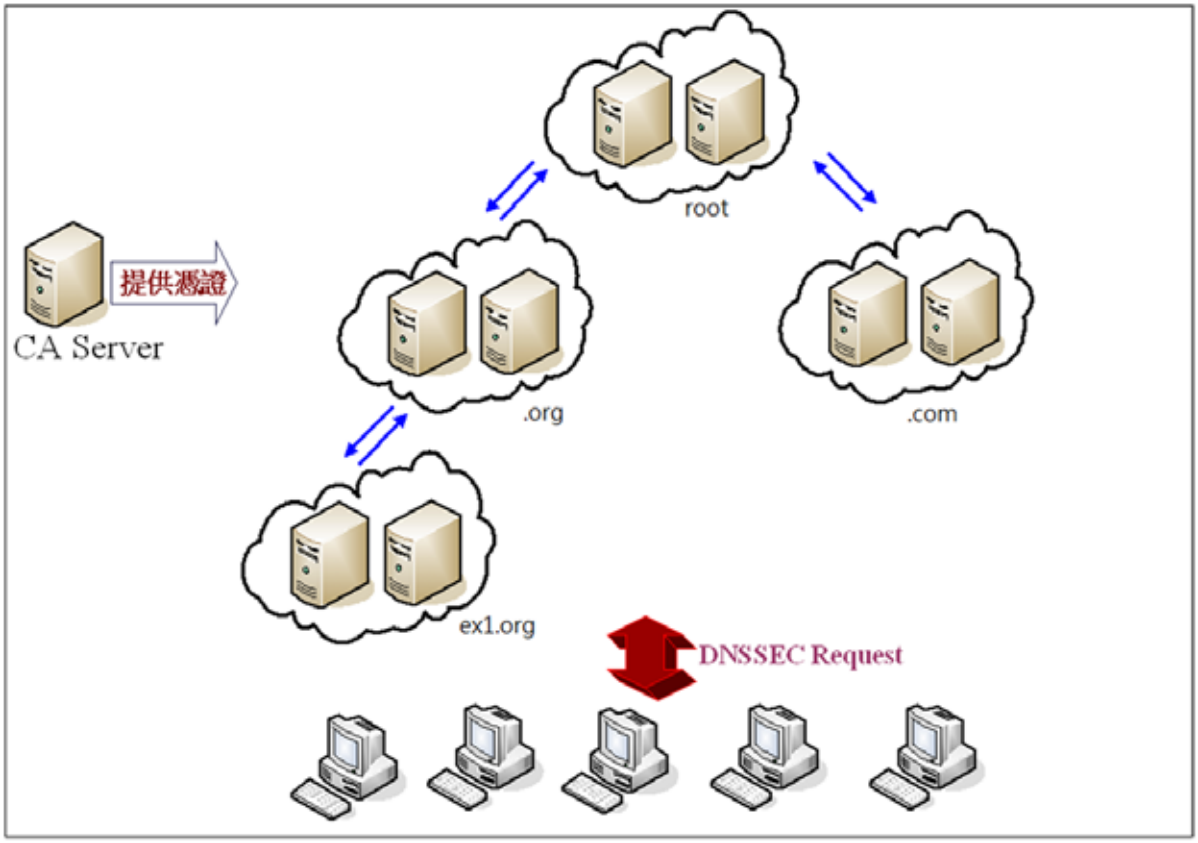

圖11 DNSSEC 實驗平台架構

在伺服器端，我們採用了 9 台 Ubuntu 10.04srv，並安裝 BIND 提供 DNSSEC 服務。在用戶端，我們採用多台 PC，安裝 Windows 7 及 Ubuntu，用以發出 DNSSEC request。為了達成整個架構的信賴鏈關係，我們需要創造多把 key pair 分屬不同伺服器，並透過適當的交換與管理，串聯起 DNSSEC 的安全機制。而用戶端必需取得 root 的 DNSKEY，就可以信賴所有的 DNSSEC 伺服器。

在這樣的實驗平台之下，已具體而微的模擬了現實的網路環境，同時我們也能夠模擬真實網路發出等量的 DNSSEC 封包。我們在這個環境執行包括 DNSSEC IPv6 實驗、中文網域實驗、憑證散佈實驗等等，實驗結果可視為與真實網路環境等價。同時我們也在此平台上進行軟體開發。

圖12 DNSSEC 實驗室實況

8. 結語

在這份文件中，我們對於 DNSSEC 近期的發展、背景知識研建測試及安全性做全面性的研究與探討，發現從根網域（root domain）到各國網路方面，各網域導入 DNSSEC 的狀況相當踴躍;除了網域的部屬外,也有許多支援的軟體,如 Bind、Ubuntu、Win7、Firefox…等。另外，DNSSEC 也針對 DNS 安全性做補強，增加了認證的功能，不僅是在解析網域名稱的過程中加上驗證的機制，也可以用來擺放憑證，此功能也間接保證了 Global PKI 的機制，可以說讓安全層級多一道保障，就能大幅提升整個 TCP/IP 網路的安全性。

另外，我們也就未來可能發展的 IPv6 及中文網域名也有做幾項實驗，確認在 DNS 升級為 DNSSEC 後，對於 IPv6 及中文化網域名是完全相容且可以實現的，這也確保了 DNSSEC 未來的發展性。

DNSSEC 的部署將被網路服務提供商視為未來網路基礎建設的重要目標，另一方面它在近年熱門的雲端運算(Cloud Computing)技術中也扮演著重要的角色，一旦所有服務都遷移到雲端，使用者獲得服務的首要步驟即是透過 DNS 服務轉譯，因此 DNS 的攻擊將造成服務中斷或惡意服務轉向。可見將傳統 DNS 升級為 DNSSEC，已成刻不容緩的任務。也因此，我們可以說 DNSSEC 是個潛力無窮並可深度發展的技術。