Email Technical Document

郵件 SPF、DKIM、DMARC 最佳化設定

防止電子報誤判成垃圾郵件

(202412)

郵件技術白皮書

沛盛資訊

沛盛資訊有限公司
台北市內湖區瑞光路 188 巷 46 號 5 樓
(02)7720-1866
contactus@itpison.com
https://www.itpison.com

目錄

1. 郵件 DNS 快速設定整理 5
   1.1. 基礎設定 5
   1.2. 完整設定 5
2. 郵件 SPF、DKIM、DMARC 設定原因 7
   2.1. 為何需要設定 7
   2.2. 郵件如何傳遞 7
   2.3. SPF 8
   2.4. DKIM 8
   2.5. DMARC 9
   2.6. SPF、DKIM、DMARC 協同運作機制 9
3. 選定域名 10
   3.1. 選定發送電子報網域 10
   3.2. 採用電子報專用域名 10
   3.3. 採用子網域 10
4. SPF 設定 12
   4.1. 通用型設定 12
   4.2. 嚴謹型設定 12
   4.3. 使用巨集設定 13
   4.4. [進階] SPF 通過判定 13
   4.1. SPF 移除 gmail “透過” 13
5. DKIM 設定 14
   5.1. 沛盛 DKIM 設定 14
      5.1.1. 2048 bit 14
      5.1.2. 1024 bit 15
   5.2. 企業自定 DKIM 16
      5.2.1. DKIM 私鑰 16
      5.2.2. Selector 子網域 17
      5.2.3. **DKIM 公鑰** 17
6. DMARC 設定 18
   6.1. 設定 DMARC 18

6.2. 解析 DMARC 統計報表 18
6.2.1. rua 與 ruf 參數 18
6.2.2. 解析 xml 檔案 18
6.2.3. DMARC 一致性判別 19
7. 追蹤連結網址設定 20
7.1. 追蹤連結設定原因 20
7.2. 追蹤連結設定做法 20
7.3. 追蹤連結設定說明 20
7.4. 追蹤連結網址需使用 SSL 21
7.4.1. 官方網站 SSL 與點擊不同 21
7.4.2. 追蹤網域 SSL 購買與安裝 21
8. MX 設定 22
8.1. 反查寄件人 22
8.2. 退信網域 22
9. 退信網域 23
9.1. 寄件者與寄件人差別 23
9.2. 選定退信網域 24
9.2.1. 電子報寄件地址 edm@example123.com 24
9.2.2. 電子報寄件地址 edm@edm.example123.com ..... **錯誤! 尚未定義書籤。**
9.3. 退信網域 DNS 設定 24
9.4. 新增之退信網域 25
9.5. 專屬退信信箱 25
10. 郵件 DNS 設定驗證 27
10.1. 使用網頁式工具驗證 27
10.2. 使用 nslookup 查詢 28
10.3. 驗證設定內容 29
10.3.1. 使用 Gmail 驗證 29
10.4. 使用第三方網頁驗證 30
10.5. d 31
11. Google 電子郵件寄件者指南 31
11.1. 大量電子郵件寄件者指南 31

11.1.1. Google 與 Yahoo 官方文件 31
11.1.2. 簡化取消訂閱 31
11.2. Google 郵件管理者工具 32
11.2.1. SPF、DKIM 和 DMARC 是否正確設定 32
11.2.2. 寄件網域的信賴程度 32
11.2.3. 寄件 IP 信賴程度 33
11.2.4. 寄件人郵件是否被檢舉 33
11.2.5. 其餘指標 33
12. 網域設定示範 34
12.1. PCHOME DNS 設定 34
12.1.1. 管理 DNS 設定 34
12.1.2. 設定主網域郵件 DNS 34
12.1.3. 設定在子網域 35
12.2. CPANEL 網域管理平台 DNS 設定 36
12.2.1. 管理 DNS 設定 37
12.2.2. 設定郵件 DNS 37

1. 郵件 DNS 快速設定整理

以下為透過「沛盛資訊」發送郵件，電子報寄件人地址：edm@example123.com，針對網域名稱 example123.com 進行設定，請將該網域置換為貴公司網域名稱，完整項次說明請參考本文各章節。設定前，請先檢查網域不在黑名單資料庫中：https://global.sitesafety.trendmicro.com/

1.1. 基礎設定

	網域	內容	類型	說明
1	(example123.com)	v=spf1 include:spf.neweredm.com a mx ~all	TXT	SPF
2	s1024._domainkey.example123.com	k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC5T4C4tyHsrVyiFZcqw4DGRDgfqtaPhEYqFSz/FSvVJywU1pBNF3rWkaaOjrzEIIb1vcIydgGi7xSXGbPqof9AnTHgVbX2cIASW09fTwTLokzj0dZ9gx9/Lsy7mjNvna4JQhLGl25oFsv2x3fwoRoynTw+2B9bRzCbTwtGX9mWOwIDAQAB;	TXT	DKIM (需同一行，不可斷行、空白)
3	_dmarc.example123.com	v=DMARC1; p=reject; pct=100;	TXT	若 DMARC 不通過 100%拒絕
若原本 example123.com 沒有 MX 才設以下				
4	example123.com	mx1.newermail.com mx2.newermail.com	MX	
5	a. 設定 Google Postmaster (寄件人工具) https://www.gmail.com/postmaster/ b. 參考 Google 大量電子郵件寄件者指南 https://support.google.com/a/answer/81126?hl=zh-Hant			

1.2. 完整設定

多數發電子報品牌，僅需基礎設定。在與「沛盛資訊」討論過後，若有需要才做完整設定。

	設定原因	域名	型態	內容
1	SPF	example123.com	TXT	v=spf1 include:spf.neweredm.com a mx ~all
2	DKIM	s1024._domainkey.example123.com	TXT	參考上表
3	DMARC	_dmarc.example123.com	TXT	v=DMARC1; p=none;rua=mailto:dmarc-admin@example.com
4	點擊追蹤	edm.example123.com	CNAME	hl.itpison.com或 專用沛盛子網域xyz.itpison.com

若原本example123.com沒有MX才設以下5、6項				
5	驗證寄件人	example123.com	MX	mx1.newermail.com mx2.newermail.com
6	a. 設定 Google Postmaster (寄件人工具) https://www.gmail.com/postmaster/ b. 參考 Google 大量電子郵件寄件者指南 https://support.google.com/a/answer/81126?hl=zh-Hant			
退信網域 edm.example123.com (選項, 有需要才設定)				
7	退信網域等同於沛盛子網域(若已設定點擊追蹤可不設)	edm.example123.com	CNAME	專用沛盛子網域
8	SPF	edm.example123.com	TXT	v=spf1 include:spf.neweredm.com a mx ~all
9	退信服務器	edm.example123.com	MX	mx1.newermail.com mx2.newermail.com

2. 郵件 SPF、DKIM、DMARC 設定原因

2.1. 為何需要設定

台灣各領域規模最大的企業，電子報幾乎都是透過「沛盛資訊」所發送。客戶在透過正規獲取的客戶郵件名單並發送行銷電子報，最常遇到的問題就是行銷電子報被判定成垃圾郵件。以國際間對垃圾郵件有許多規範，但採用合法獲得的會員名單，並透過像「沛盛資訊」這樣正規電子報發送業者，發送行銷宣傳郵件是被國際認可的行銷行為。但若是客戶不了解國際間在對電子報防範濫發所設定的機制，沒有進行適當的設定，行銷宣傳電子報就容易被判定為垃圾郵件。

國際間相關組織制定了防治濫發垃圾郵件，制定了許多做法，除了在法律層面各國立法外，在國際間的郵件交換協定上，訂出了 SPF、DKIM 以及 DMARC 等規範。收信服務器如 Gmail、Yahoo、Hotmail 等，在收郵件時會去檢查這些規範有無被加入，如果沒有的話被判定成垃圾信的可能性大幅提高。對合法的電子報行銷郵件，「沛盛資訊」建議發信者都加入這些郵件安全性機制，以降低被判成垃圾信的可能。

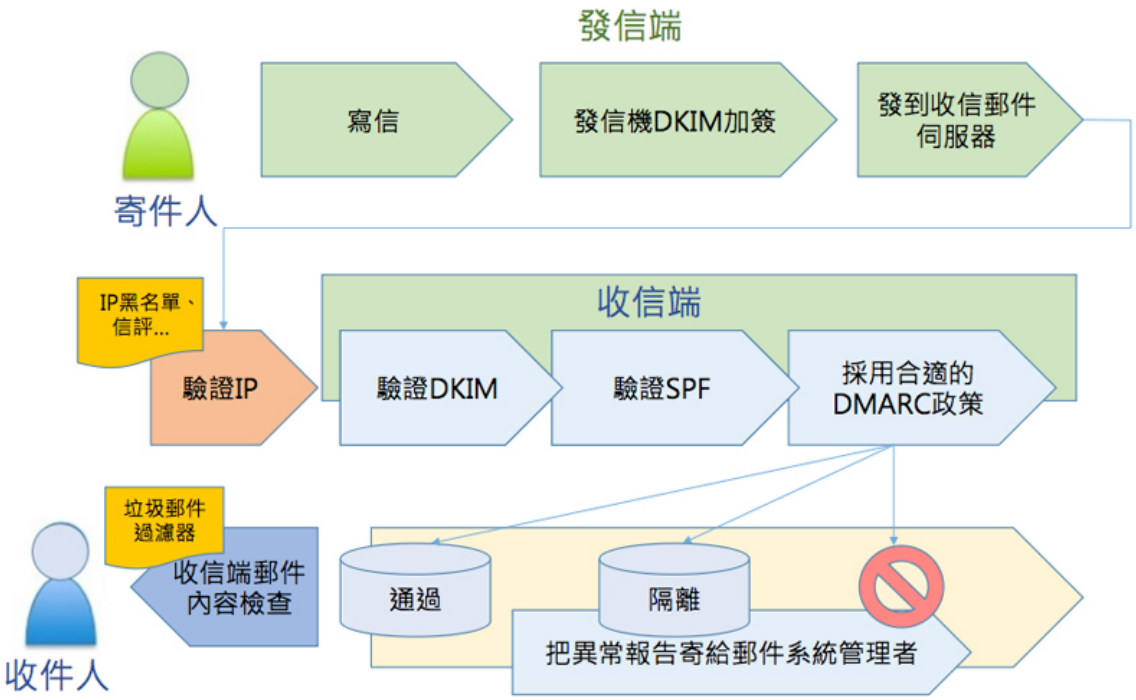
本郵件技術白皮書將以沛盛多年實務經驗，詳細說明企業如何進行電子報的 DNS 設定，主要是 SFP、DKIM 以及 DMARC，並額外介紹在設定電子報 DNS 的技巧。

2.2. 郵件如何傳遞

我們透過以下這張圖片，來解說 SPF/DKIM/DMARC，如何在一封郵件發信與收信中發生作用。

首先，寄信人寫完電子郵件按下發送後，這封郵件在發信服務器端進行 DKIM 加簽(加入私鑰)，確保過程不會遭到竄改。接下來傳送到收信端服務器，此時會先檢查發信機的 IP 是否可靠，有沒有在濫發郵件黑名單，在國際間有專門組織發佈濫發黑名單 IP 地址。通過之後收信服務器接著檢查 DKIM(公鑰)，看是否跟原本加簽的私鑰相符。之後驗證 SPF，這是檢查寄信者的網域，是否有同意這個發信 IP 去發信。

接著進行 DMARC，也就是說前面的 SPF/DKIM 檢查若有錯誤，這封郵件可以依舊發送、隔離(通常就是標注為垃圾郵件)，或是拒收。然後郵件才傳給收信程式(例如 Gmail 網頁介面，或 Outlook)，此時檢查內文看是否可能為垃圾信件(例如：大促銷、大降價等文字)。



原圖來自dmarc官網https://dmarc.org/，此為中譯方便理解。

2.3. SPF

SPF (Sender Policy Framework) 寄件者政策框架，用來規範在選定的郵件發送服務器位址，可以用來發送寄件人的網域郵件。這樣機制可以避免垃圾信濫發業者，偽裝網域發送假冒郵件。SPF 的設定裡面，列出明確許可的郵件發信機網域名稱，郵件收信服務器透過檢查發信人網域的 SPF，就知道這封電子郵件是否來自被允許的發信機位址。

SPF 官方網站 http://www.open-spf.org/

2.4. DKIM

DKIM (DomainKeys Identified Mail)，網域驗證郵件，是一種電腦數位簽章，採用公鑰與私鑰這種加密驗證法進行。在發送郵件時由發信服務器對郵件以私鑰進行簽章，而在郵件接收服務器上，會透過 DNS 到發信者的網域查詢 DKIM 紀錄，擷取上面記載的公鑰資料，然後對這封郵件做簽章解碼，如果公鑰與私鑰能配對成功，代表郵件確實為原始發信機所發出。

透過 DKIM 的導入，收信郵件服務器可以驗證郵件絕對是原本的郵件發信服務器所發出，而且在郵件複雜的傳送過程中，這封郵件內容也毫無被竄改過，這杜絕了濫發垃圾信業者，透過假冒的郵件發送機以及假冒的私鑰簽章寄送垃圾信。由於係採用公鑰與私鑰簽章架構，因此除了在網域做 DKIM 設定之外，在郵件發信服務器上也要進行對應的私鑰設定。

DKIM 官方網站 https://dkim.org/

2.5. DMARC

DMARC (Domain-based Message Authentication,Reporting & Conformance)，用來輔助 SPF 與 DKIM 的不足，用來讓發信端網域通知收件端郵件服務器，當遇到 SPF 與 DKIM 的設定檢查不過時，進行的處理方式。最知名的案例就是 Yahoo 在 2014 年，宣布 DMARC 設為「拒絕」，也就是說所有不是從 Yahoo 郵件服務器發出的郵件，寄信人都不能用 Yahoo 郵件地址。

由於企業的郵件架構可能極為複雜，以 DKIM 設定還要發信端服務器配合設定，某些企業郵件可能透過當地 ISP 做為郵件發信機，但這也是合法的郵件。由於真假不一，收信端很難知道遇到 SPF/DKIM 驗證不過該拒絕還是放行。但假若寄件者絕對知道所有的郵件都一定符合 SPF/DKIM 驗證，寄件方就可以透過 DMARC 通知收件方郵件服務器，遇到驗證不過時的處理方式(通過/隔離/拒絕)。

DMARC 官方網站 https://dmarc.org/

2.6. SPF、DKIM、DMARC 協同運作機制

透過 SPF、DKIM、DMARC 的郵件驗證機制，在收件端郵件服務器，首先由 SPF 可以檢查是否發信機的 IP 為認可發送該寄信者網域郵件。其次，以 DKIM 查看郵件發信時的私鑰與收信時的公鑰是否匹配，代表內容確實為該發信機發出。最後，由 DMARC 知道，假設 SPF/DKIM 驗證不過時，此封郵件該如何處理。以 Gmail 為例，必須做到 SPF、DKIM、DMARC 通通都設定且驗證通過，這封郵件才比較不可能被丟進垃圾信箱匣(另外還牽涉到郵件內文等)。

3. 選定域名

3.1. 選定發送電子報網域

透過「沛盛資訊」作爲電子報發送端，在設定郵件 DNS 之前，首先要決定要用來發電子報的域名。「沛盛資訊」建議分開公司原本域名跟電子報發送的域名，例如公司名稱為 example.com，電子報寄件人則用 example123.com。

將電子報發信網址與原本公司網址分開，這是因為電子報的發送量大，有可能發信域名的 IP 信評會受到不同層度的影響，為了避免發送電子報反而影響到公司原本正常使用的網域名稱信評，可能進而影響到員工郵件信箱發送，因此將電子報發送使用的域名與公司原本域名分開。

了解電子報寄件人網域要與原本公司網域分開的原理，在實務上以「沛盛資訊」的經驗，我們的企業客戶會採用兩種方法進行：

3.2. 採用電子報專用域名

做法：原本公司網域 example.com，電子報發信人的網域為 example123.com。

原因：這樣的設定方法，收信的讀者足以辨認出這封電子報，是由原本 example.com 這間公司所發出。而電子報所使用的網域，又不會影響到原本公司網域的信評，此種作法為 90%的國內外大企業所採用

本文以下範例為電子報採用專有域名方式 example123.com，並使用電子報寄件者 edm@example123.com 為例做介紹。

3.3. 採用子網域

做法：原本公司網域 example.com，電子報發信人的網域為 edm.example.com。
原因：有些類型的企業，希望保有公司對外統一形象，或者其它原因要求一定要使用公司原本網域名稱，這時候建議採用發送電子報專用的子網域名稱。由於設定電子報發送需要在 DNS 進行許多設定，這種作法對原本公司網域 example.com 的 DNS 不需做任何變動，只需要在子網域 edm.example.com 進行相對應的郵件 DNS 設定。
應用：「沛盛資訊」某客戶為跨國知名金融集團，透過電子報系統對它的全球客戶發送金融研究報告，屬於大量發送郵件但非行銷型電子報，因此要保留原有公司的網域名稱，便採用這種子網域的做法，針對子網域做所有 DNS 郵件最佳化設定。

若欲使用子網域作為電子報發送網域，所有設定方法同本文設定描述，惟須設定在子網域之上。

以 edm.example.com 作為電子報發送子網域為例，所需使用完整網域分別為：

- SPF: edm.example.com
- DKIM: s1024._domainkey.edm.example.com
- DMARC: _dmarc.edm.example.com

4. SPF 設定

4.1. 通用型設定

請檢查寄件人信箱網域(example123.com)，在 DNS 裡是否有 SPF 的 TXT 紀錄，若原來沒有 SPF（TXT）記錄，請新增一筆紀錄如下，若原來已有紀錄請將以下增加至原來 SPF 紀錄。

include:spf.neweredm.com

若原有 SPF 已經有 include 其它網域，則新增另一則 include 即可：

v=spf1 include:_spf.google.com include:spf.neweredm.com a mx ~all

電子報寄件人為 edm@example123.com，則為檢查 example123.com 的 DNS 裡面 TXT 記錄。

記錄名稱	Type	文字(TXT 值)
example123.com	TXT	v=spf1 include:spf.neweredm.com a mx ~all

說明：

(1) v=spf1 表示 spf 所使用的版本。

(2) include 表示授權給該郵件伺服器。

(3) a 表示比對 DNS 紀錄中的"A"紀錄，允許在"A"紀錄裡面的 IP 為發送郵件來源 IP。

(4) mx 表示比對 DNS 紀錄中的"MX"紀錄，允許在"MX"紀錄裡面的網域為發送郵件來源網域。

(5) ?all 表示對非 SPF 表列 IP 發送位址，不做成功失敗判定。

4.2. 嚴謹型設定

對於原本已有設定 SPF 企業，「沛盛資訊」提供另一組「_spf.neweredm.com」供使用，結尾設定為 ~all。

記錄名稱	Type	文字(TXT 值)
example123.com	TXT	v=spf1 include:_spf.neweredm.com a mx ~all

與前一組「spf.neweredm.com」設定結尾設定為 ?all 差別如下：

- ~all：凡發信 IP 位址不在 SPF 表列中，判定為 soft fail，相當於不通過。
- ?all：凡發信 IP 位址不在 SPF 表列中，不做通過或不通過判定。

若非對 SPF 設定極為熟悉，建議以「spf.neweredm.com」設定。

4.3. 使用巨集設定

對於大型企業有複雜內部跟外部發信服務器造成 spf 過長或是由於資安考量，則可透過巨集(macro)語法進行設定。詳細用法請參考 SPF RFC7028 Session 7.2。

例如，若要允許透過 61.218.77.160 以及 61.218.77.161 發信，於 SPF 使用%{i} (該封郵件寄件來源 ip)，在 DNS 中加入以下 SPF:

sample123.com IN TXT "v=spf1 exists:%{i}._spf.example.com -all"

同時將 61.218.77.160 以及 61.218.77.161 加入 DNS:

61.218.77.160._spf. sample123.com IN A 127.0.0.2
61.218.77.161._spf. sample123.com IN A 127.0.0.2

4.4. [進階] SPF 通過判定

收信服務器判定是否通過 SPF，係以退信網域(return-path)而非寄件人網域(example123.com)。若沒有特別設定使用退信網域，使用「沛盛資訊」發送均會採用 newermail.com 作為收取退信使用。而 newermail.com 都已經設定完成 SPF，因此 SPF 會判定通過。

本文建議客戶除了設定寄件人網域(example123.com) SPF，並與「沛盛資訊」討論是否要設定退信網域，可提升整體信件可信度，對降低垃圾信判定帶來幫助。

4.1. SPF 移除 gmail “透過”

透過沛盛資訊或第三方電子報系統發郵件到 Gmail，若沒有設定 spf，在收信時會顯示”透過, via” ，對大品牌而言，容易讓收信人覺得並非真實是這企業所發出。在設定完 spf 之後，此一”透過”訊息便會移除。

5. DKIM 設定

5.1. 沛盛 DKIM 設定

重要：DKIM 設定完畢後，請務必通知「沛盛資訊」（沛盛系統也須對應設定私鑰）

以電子報寄件人為 edm@example123.com，增加一筆 TXT 紀錄：

5.1.1. 2048 bit

記錄名稱: s2048._domainkey
文字(TXT 值):
"k=rsa;
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA3ML5/DmtZsycBADbO3
v2sYDAXkSus6FO5l5S6mmn5Xswx7I2j6X++"
"7PUt6dj490Og0Co5QmpWT3CblgWbVV1nczwbIhojoXFempnEXP5yH9AF5A9DqxZrQ7zv
/Wp+st8P1vFIDnrkXRKDL4wsRdhWc0JbtzRzUD"
"mhNCsKXVFoTjNtrv/tXW5OTy/iaP8fUzdl9msFxuN5C+WJTx590MFs4eXKoRXRsDdJt3qi
RqNRVPKbTXKoJsrkSyYxKvTC4bk9oF01HB/"
"cKDtbmKIaXzor4yAm/XrpkIce7ufJFMiMbPs5e4G0v9daU6xQDXhpGyeM3uBgMSF/lxlLj6
vDbJHrwIDAQAB;"

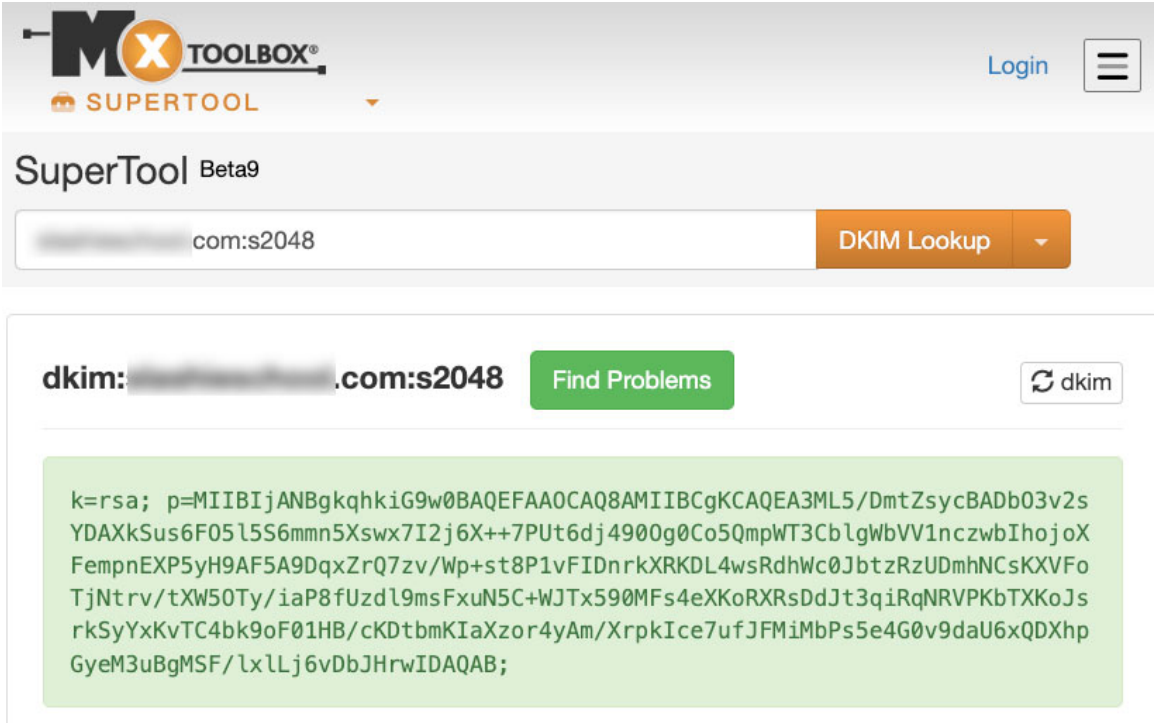
說明:
(1) 由於 2048 bit 的長度，會超過多數 DNS 服務器對 TXT 長度限制(256 字元)，因此上述 DKIM 被拆分成四部分，以引號 ” 在字串前後。
(2) s20484 稱為” selector” ，為 DKIM 識別名稱。
(3) k 為加密演算法，預設為 rsa。
(4) p 為公鑰內容(public key)。
(5) 開頭可加入” v=DKIM1;” ，這是預設值，若沒寫則使用預設。
註：分號 “;” 為 DKIM 用來區分不同設定數值。

設定範例

Type	Name	Priority	Content	TTL
TXT	s2048._domainkey	0	"k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA3ML5/DmtZsycBADbO3v2sYDAXkSus6FO5l5S6mmn5Xswx7l2j6X++" "7PUt6dj490Og0Co5QmpWT3CblgWbVV1nczwblhojoXFempnEXP5yH9AF5A9DqxZrQ7zv/Wp+st8P1vFlDnrkXRKDL4wsRdhWc0JbtzRzUD" "mhNCsKXVFoTjNtrv/tXW5OTy/iaP8fUzdl9msFxuN5C+WJTx590MFs4eXKoRXRsDdJt3qiRqNRVPKbTXKoJsrkSyYxKvTC4bk9oF01HB/" "cKDtbmKlaXzor4yAm/XrpkIce7ufJFMiMbPs5e4G0v9daU6xQDXhpGyeM3uBgMSF/lxlLj6vDbJHrwIDAQAB;"	14400

▲ 於 DNS 服務器中，加入 s2048 bit DKIM 範例。字元中以引號分為四段。

驗證 DKIM，可使用 mxtoolbox.com 做驗證
https://mxtoolbox.com/SuperTool.aspx



5.1.2. 1024 bit

對大多數的客戶，為了增強資安防護，建議使用 2048 bit DKIM。但若是在所使用的 DNS 服務器上，無法建立 2048 bit DKIM，可使用強度較低之 1024 bit DKIM。

記錄名稱: s1024._domainkey
文字(TXT 值):
k=rsa;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC5T4C4tyHsrVyiFZcqw4DGRDgfqtaPhEYqFSz/FSvVJywU1pBNF3rWkaaOjrzEIIb1vcIydgGi7xSXGbPqof9AnTHgVbX2cI

ASW09fTwTLokzj0dZ9gx9/Lsy7mjNvna4JQhLGl25oFsv2x3fwoRoynTw+2B9bRzCbTwtGX9mWOwIDAQAB;

```
k=rsa;  p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC5T4C4tyHsrVyiFZcqw4DGRDgfqt
```

說明:

(6) s1024 稱為”selector”，為 DKIM 識別名稱。

(7) k 為加密演算法，預設為 rsa。

(8) k=rsa; p=MIG….整串內容,並且整串不能有斷行。

(9) p 為公鑰內容(public key)。

(10) 開頭可加入”v=DKIM1;”，這是預設值，若沒寫則使用預設。

註：分號 “;” 為 DKIM 用來區分不同設定數值。

範例：以「沛盛資訊」itpison.com 網域為例，使用 nslookup 解析出來成功的畫面

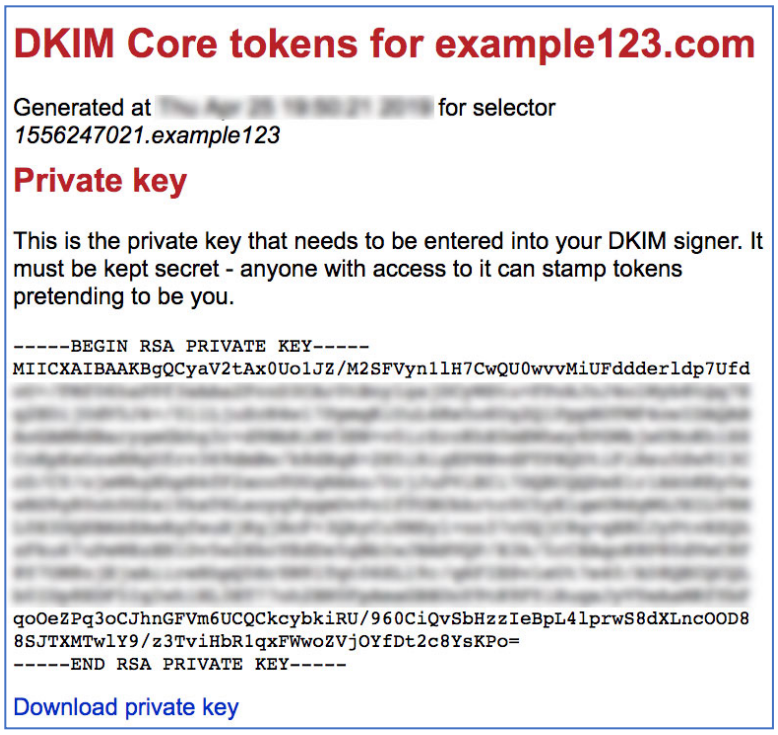
5.2. 企業自定 DKIM

對於大型企業通常想要用自己的 DKIM，可以在以下 DKIM 官方網站自行建立：
https://dkimcore.org/tools/

若以 example123.com 為範例，生成 DKIM:

5.2.1. DKIM 私鑰

生成後的 DKIM Private Key(私鑰)如下圖。這串的私鑰需提供給「沛盛資訊」，在郵件發送時加入專屬私鑰。



DKIM Core tokens for example123.com

Generated at [redacted] for selector *1556247021.example123*

Private key

This is the private key that needs to be entered into your DKIM signer. It must be kept secret - anyone with access to it can stamp tokens pretending to be you.

```
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQCyaV2tAx0Uo1JZ/M2SFVyn1lH7CwQU0wvvMiUFddderldp7Ufd
[redacted]
qoOeZPq3oCJhnGFVm6UCQCkcybkiRU/960CiQvSbHzzIeBpL4lprwS8dXLncOOD8
8SJTXMTwlY9/z3TviHbR1qxFWwoZVjOYfDt2c8YsKPo=
-----END RSA PRIVATE KEY-----
```

Download private key

5.2.2. Selector 子網域

上圖生成出了一個 DKIM 的 selector:

1556247021.example123

在這樣的 selector 之下，整個 DMIM 子網域設定，就跟前一章節使用沛盛的 DKIM 設定不同，以此範例(每次生成會不同)的 DKIM 子網域：

1556247021.example123._domainkey.example123.com

5.2.3. **DKIM 公鑰**

生成私鑰之後可看到公鑰，這是要設定到 DNS 上，作為 DKIM 值：

```
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCyaV2tAx0Uo1JZ/M2SFVy
n1lH7CwQU0wvvMiUFddderldp7UfdoU+/FMf06haPPf3xAAa2FcnD3CAr0t
BnylgajDCyWStu+FPokJnJ4olWyb8tQq7Eq2EOijUdV5J4+/0l1LjuZcN4w
17PpmqKiUuL4Ke5o6Ug2Q1PppHOTWF4owIDAQAB
-----END PUBLIC KEY-----
```

```
k=rsa;  p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCyaV2tAx0Uo1JZ/M2S
```

同樣 p 之後的 DKIM 公鑰是不能有斷行。

6. DMARC 設定

6.1. 設定 DMARC

同樣以電子報寄件人為 edm@example123.com，增加一筆 TXT 紀錄：

記錄名稱	Type	文字(TXT 值)
_dmarc.example123.com	TXT	v=DMARC1; p=reject; pct=100;

DMARC 如何判定通過，可參考以下 DMARC Alignment 說明。

說明：
(1) v 表示 DMARC 版本。
(2) p 表示採用的處理方式，p=reject 拒收該郵件，p=none 表示不攔阻將郵件傳送到信箱，p=quarantee 代表標注垃圾信後放行郵件。
(3) pct=100 代表郵件 100%都經由此條件做判斷。
(4) 務必設好 SPF 及 DKIM 之後，才可設定此 DMARC 紀錄，否則發出之郵件都會被拒收。

6.2. 解析 DMARC 統計報表

6.2.1. rua 與 ruf 參數

公司的 MIS 部門若有解析 DMARC 所產生的統計報表，也可設定 rua 與 ruf 兩個參數：
v=DMARC1; p=none; rua=mailto:dmarc-aggregate@example.com; ruf=mailto:dmarc-afrf@example.com

rua 表示 DMARC 統計報表 XML 寄送信箱，此處請改為電子報發件方系統管理者真實信箱。
ruf 表示將這封發生錯誤的郵件留存為證據，此處請改為要保留該證據的收信信箱。

6.2.2. 解析 xml 檔案

透過 rua 所收到的問題統計報表，採用 XML 格式，請參考沛盛網站 DMARC 報表 XML 範例:
https://www.itpison.com/newitpison/download/dmarc-rua-report.xml
也有許多網站可以協助產出解析報表如

- https://easydmarc.com/
- https://mxtoolbox.com/

6.2.3. DMARC 一致性判別

DMARC 判定標準稱為 DMARC 一致性(DMARC Alignment) 或 DMARC identifier alignment，是判定以下兩者至少其中一項通過：

1. 條件 A：寄件人 from 與退信網域(Return-path)相同，且退信網域已設定 SPF
2. 條件 B：寄件人 from 網域與 DKIM 網域相同，且有 DKIM 加密。

條件 A 的判定，電子報寄件人為 edm@example123.com 若無設定退信網域，則採用 newermail.com 作為退信網域，SPF 判定係根據退信網域 newermail.com。此部分由於寄件人網域 example123.com 與退信網域不同，DMARC Alignment 判定會不通過。

條件 B 的判定，寄件人網域與 DKIM 網域一致，均為 example123.com。DMARC Alignment 判定通過。

DMARC Alignment 判定係兩項條件取其一，若未設定退信網域，將由條件 B 判定通過，因此 DMARC Alignment 通過。

條件	寄件人網域	退信網域	DKIM 網域	DMARC 判定
A	example123.com	newermail.com	example123.com	No 寄件人與退信不同網域
B	example123.com	newermail.com	example123.com	Yes 寄件人與 DKIM 同網域

7. 追蹤連結網址設定

7.1. 追蹤連結設定原因

「沛盛資訊」提供點選電子報連結紀錄，包含哪些客戶點了這些連結、點選的時間及次數、以及哪些產品連結最受客戶的青睞。追蹤點擊連結的做法如以下圖示:

以上圖而言，電子報的內文連結原本到 tw.yahoo.com，但是為了進行點擊追蹤，點擊的連結會先到 hl.itpison.com(「沛盛資訊」服務器)，進行點擊統計，之後再轉到原本的 tw.yahoo.com。

以電子報發信人 edm@example123.com 為例，電子報內追蹤連結網址會出現 https://hl.itpison.com/hl/…./xxx.htm。
對品牌大廠而言，整封電子報的連結應該都是要自己的網域名稱才合適，而且出現其它的域名，也會降低電子報信用等級，增加進入垃圾信匣的可能性。因此，可以進行 DNS 的設定，讓追蹤連結網址出現自己的網域，如 https://edm.example123.com/HL/…/xxx.htm

7.2. 追蹤連結設定做法

以電子報寄件人為edm@example123.com，請新增以下子網域(或其它合適子網域名稱)：

edm.example123.com

接著可以透過DNS的CNAME作設定:

記錄名稱	Type	文字(TXT值)
edm.example123.com	CNAME	hl.itpison.com (或沛盛專機子網域)

7.3. 追蹤連結設定說明

CNAME（Canonical Name Record）別名記錄：

將 edm.example123.com 設一個 CNAME 到 hl.itpison.com (或「沛盛資訊」所提供專屬子網域)，再透過電子報後端程式的轉換，圖片中的追蹤連結網址就會變為 https://edm.example123.com/hl/…/xxx.htm

CNAME 的設定就是讓網域有別名，亦即上述 edm.example123.com 等於 hl.itpison.com (或「沛盛資訊」所提供專屬子網域)。

7.4. 追蹤連結網址需使用 SSL

由於資訊安全越來越受重視，瀏覽器已全面對未使用 SSL 網域發出警示，使用者會對該網域產生疑慮，而不前往瀏覽，因此所有網域都應使用 SSL，用來做點擊追蹤網域也同樣應該配置 SSL。

7.4.1. 官方網站 SSL 與點擊不同

企業客戶大多了解官方網站網域需用 SSL，例如 https://www.example123.com。但網域 SSL 的使用是要設定在每個子網域，亦即官網所用 SSL，並不能應用在追蹤網域 edm.example123.com，除非官網購買的為全域通用，子網域也可使用，否則就需要另外購買該子網域 SSL。

7.4.2. 追蹤網域 SSL 購買與安裝

追蹤網域 edm.example123.com 需安裝在「沛盛資訊」服務器上，並作適當設定才能生效。為了提供客戶一站式服務，可於「沛盛資訊」購買 SSL，請與業務人員聯繫方案價格。

註: 設定完 CNAME 後，也請通知「沛盛資訊」在電子報系統後台進行對應啟動才正式生效。

8. MX 設定

8.1. 反查寄件人

電子郵件在傳送時，收信端服務器會透過 MX 記錄，反查原本發信人郵件地址是否真實存在，不是虛假郵件地址。

以電子報寄件人為 edm@example123.com 為例，收件服務器的作法，會檢查 example123.com 的 DNS 中 MX 紀錄中郵件服務器是否存在與是否能夠連線，並會詢問該郵件服務器，寄件人”edm”這個帳號是否存在於此服務器。

以 MX 紀錄而言，若 example123.com 原本已經設立 MX 記錄，則不用做更動。但如果 example123.com 這是專門用來發電子報的網域名稱，完全沒有用在其它地方，且該網域本身也不想要收信，可將 MX 記錄設到「沛盛資訊」郵件服務器，未來收件服務器進行 MX 紀錄反查與詢問是否寄件人帳號存在，就會回覆相對應的結果。

注意：但若原本該網域沒有用來收信，因此設定 MX 到「沛盛資訊」郵件服務器。若未來該網域變更也用來收信，則需將指向到「沛盛資訊」的 MX 刪除。

若原本 example123.com 網域的 DNS 並無 MX，加入以下 MX 記錄。
沛盛公雲客戶：

記錄名稱	Type	Record	Priority
example123.com	MX	mx1.neweredm.com mx2.neweredm.com	10

沛盛專機客戶：

記錄名稱	Type	Record	Priority
example123.com	MX	[專機子網域]	10

8.2. 退信網域

請參閱「退信網域」章節說明，退信網域亦須設定 MX，但與寄件人網域設定 MX 用途不同。

- 寄件人網域 MX：用來驗證寄件服務器與寄件人是否存在，可設定在企業自有郵件服務器，或是「沛盛資訊」郵件服務器。
- 退信網域 MX：用來接收電子報發送後退信，必須設定到「沛盛資訊」郵件服務器，並作為退信報表統計。

9. 退信網域

發送量少客戶可以不設定退信網域，但在郵件原始檔，可看到該郵件係由「沛盛資訊」處理退信。若發送大量郵件品牌企業，可設定退信網域，則在郵件原始檔，將完全看不到「沛盛資訊」郵件服務器，完全如同該企業發送網域的郵件。但理解退信網域前，需先釐清寄件者跟寄件人的不同。

9.1. 寄件者與寄件人差別

一般而言由「沛盛資訊」雲端電子報所寄出郵件，寄件人(MAIL FROM)為 mail.neweredm.com。

寄件人 FROM 並非讀信程式可見之”寄件者”。參見下圖 Gmail 收信示範，”寄件者”為讀信程式可見發信人郵件地址。”寄件人” MAIL FROM 則為郵件寄送 SMTP 服務器溝通過程所使用。

依照 SMTP 協定，退信網域(Return-path) 等同於寄件人網域 MAIL FROM (又名 bounce address, reverse path, envelope from, envelope sender, return address)

亦即若有退信，將退到此一網域特定郵件地址，如下圖此一任務發送退信將至 Return.EID44fb8629.Job@mail.neweredm.com，此退信網址為發信機自動產生。

```
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@寄件者網域.com header.s=s1024 header.b=Ku4KVjH+;
       spf=pass (google.com: domain of return.eid44fb8629.job@mail.neweredm.com
designates 61.218.78.239 as permitted sender)
smtp.mailfrom=Return.EID44fb8629.Job@mail.neweredm.com;   寄件者網域
       dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=.com
Return-Path: <Return.EID44fb8629.Job@mail.neweredm.com>
Received: from b239.neweredm.com (b239.neweredm.com. [61.218.78.239])
        by mx.google.com with ESMTPS id p35-
```

當郵件發送量大或想設定專屬退信網域作為退信，可將此”寄件者”修改成企業本身網域。例如 edm.example123.com，當電子報發送有退信時，就會將退信傳送此網域。使用 CNAME 設定 edm.example123.com 等同於「沛盛資訊」服務器後，即使郵件原始檔顯示為 edm.example123.com，但退信仍然是在「沛盛資訊」服務器。

此一設定，”寄件者”為企業自有網域，寄件人網域與寄件者網域兩者一致，也對降低判定成為垃圾信有幫助。

9.2. 選定退信網域 (return-path)

9.2.1. 電子報寄件地址 edm@example123.com

退信網域可依企業需要，自行提供子網域即可。但若企業在初期設定寄件人網域，已經設定了點擊用子網域 (e.g. edm.example123.com)，則可使用該子網域作為退信網域，或是使用明確的退信網域如 return.example123.com。

9.3. 退信網域 DNS 設定

新增退信網域 return.example123.com，需設定 MX 與 SPF，所有設定內容與主網域 example123.com 相同。

設定 SPF 原因在於收件服務器會驗證退信 SPF，需與寄件者網域 SPF 相同，因不用來發信無需加簽郵件故可不設 DKIM，亦不需設定 DMARC。設定 MX 則是委由「沛盛資訊」郵件服務器進行退信處理。此一 MX 不可設定到企業內部郵件服務器，因為這些是電子報退信，若退回企業內部服務器，由於並非由該郵件服務器發送，將無法正確處理。且由於沒有退回「沛盛資訊」郵件服務器，也無法統計退信數。

沛盛資訊雲端客戶

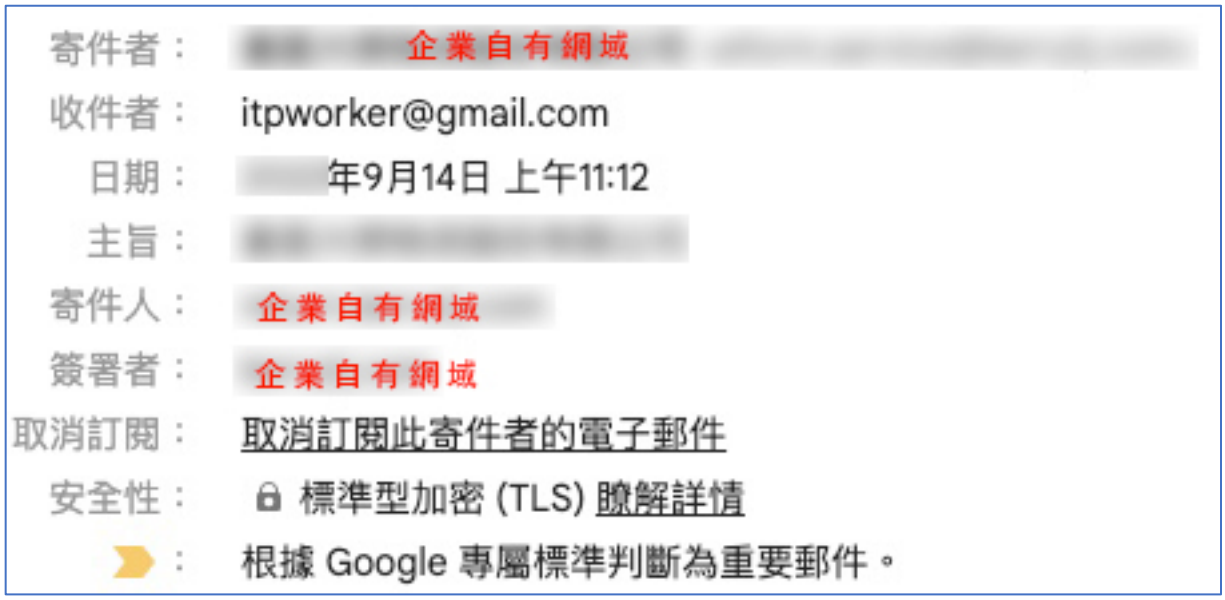
Record Name	Record Type	Value
return.example123.com	TXT	v=spf1 include:spf.neweredm.com ~all
return.example123.com	MX	mx1.neweredm.com mx2.neweredm.com

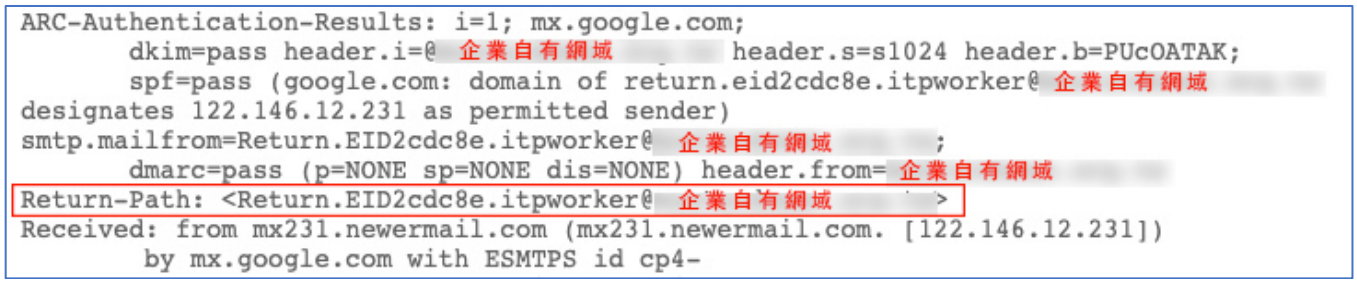
沛盛資訊專機客戶

Record Name	Record Type	Value
return.example123.com	TXT	v=spf1 include:spf.neweredm.com ~all
return.example123.com	MX	專機.neweredm.com

9.4. 新增之退信網域

經此修改後，寄件人、寄件者，以及退信網域均為企業客戶自有網域。對收信服務器能提升這封信可信度，降低退信或垃圾信判定機率。





9.5. 專屬退信信箱

以上所示以設定企業客戶自有網域為退信網域，但退信信箱係發信機依照任務自動產生，為亂數所產生之郵件地址。發送後退信回到此信箱，經統計後便會呈現在退信報表中。

針對更嚴格的寄件設定，更可修改此一亂數產生之退信信箱網址，成為特定退信信箱，如：
bounce@edm.example123.com

註：若非使用電子報專用網域，而是使用公司網域(或子網域)作為電子報發送網域，設定完退信網域後，發送到公司內部郵件有可能被封鎖，可參考此份「允許外部發送同網域郵件到公司內部」進行設定解決。

10.郵件 DNS 設定驗證

10.1.使用網頁式工具驗證

使用 https://mxtoolbox.com/ 做網頁式驗證：

1. SPF 驗證:

https://mxtoolbox.com/SuperTool.aspx (選取 SPF Record Lookup)

正確結果：

```
v=spf1 include:spf.neweredm.com a mx ptr ?all
```

備註：若 spf 有使用巨集(macro)語法，則需使用以下測試工具：

https://vamsoft.com/support/tools/spf-policy-tester

2. DKIM 驗證

https://mxtoolbox.com/dkim.aspx

正確結果：

```
k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC5T4C4tyHsrVyiFZcqw4DGRDgfqtaPhEYqFSz/FSv
```

3. DMARC 驗證:

https://mxtoolbox.com/SuperTool.aspx (選取 DMARC Lookup)

正確結果：

```
v=DMARC1; p=none;
```

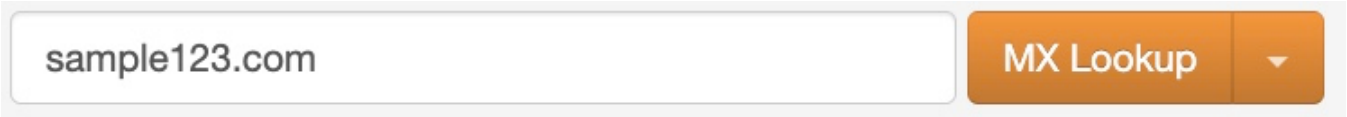
4. 若有設定點擊追蹤網址:

https://mxtoolbox.com/SuperTool.aspx (選取 CNAME Lookup)

正確結果：

Type	Domain Name	Canonical Name	TTL
CNAME	[redacted]	hl.itpison.com	60 min

5. 若有設定郵件 MX:
https://mxtoolbox.com/SuperTool.aspx (選取 MX Lookup)



正確結果：

Pref	Hostname	IP Address	TTL		
10	mx1.neweredm.com	113.196.228.10 NCIC-TW (AS9919)	60 min	Blacklist Check	SMTP Test
10	mx2.neweredm.com	113.196.228.11 NCIC-TW (AS9919)	60 min	Blacklist Check	SMTP Test

10.2.使用 nslookup 查詢

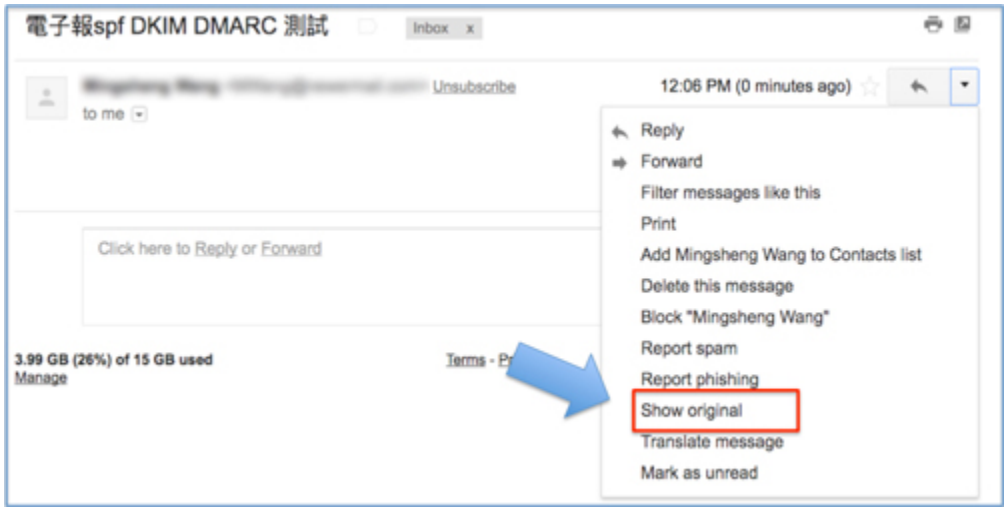
郵件 DNS 設定完畢後，可以透過 nslookup 程式下參數指令來進行 DNS 內容查詢，或者利用網路版(註 1)查詢。自有 DNS 設定完，須等待數小時對外做正式公佈，以下的查詢係透過中華電信 dns.hinet.net 來查看是否已經正式生效。

	設定原因	域名	型態	nslookup 指令
1	SPF	example123.com	TXT	nslookup -q=txt example123.com dns.hinet.net
2	DKIM	s1024._domainkey.example123.com	TXT	nslookup -q=txt s1024._domainkey.example123.com dns.hinet.net
3	DMARC	_dmarc.example123.com	TXT	nslookup -q=txt _dmarc.example123.com dns.hinet.net
4	點擊追蹤	edm.example123.com	CNAME	nslookup -q=cname edm.example123.com dns.hinet.net

10.3.驗證設定內容

10.3.1. 使用 Gmail 驗證

測試 SPF、DKIM、DMARC 有沒有設定成功，可利用「沛盛資訊」電子報發信系統，實際以電子報寄件人 edm@example123.com，發送測試郵件到 Gmail 帳號，之後登入 Gmail，如下圖指示來查看 Gmail 郵件原始檔。

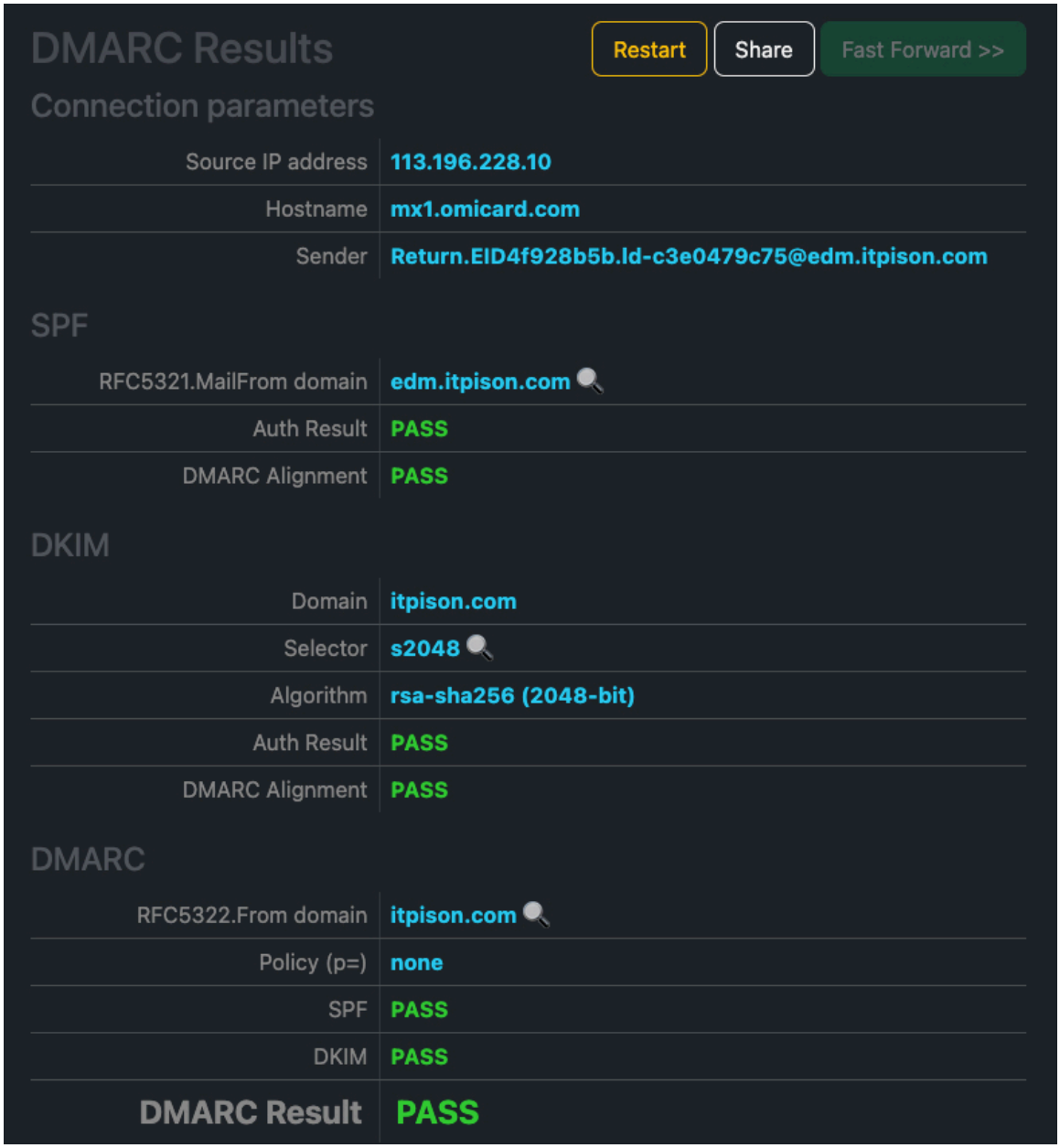


在郵件的原始檔內，就可以看到 SPF、DKIM、DMARC 是否通過的訊息，務必做到這三項設定全部都通過，整個設定才算大功告成。

10.4.使用第三方網頁驗證

可使用以下 DMARC 測試網站，只要發信到該網站首頁提供的郵件信箱，就會給詳細完整的 SPF/DKIM/DMARC 驗證報告。

https://www.learndmarc.com/



10.5.d

11.Google 電子郵件寄件者指南

11.1.大量電子郵件寄件者指南

11.1.1. Google 與 Yahoo 官方文件

為了對抗國際間垃圾信氾濫，Google 在將自 2024 年 2 月起，寄送到 Gmail 的寄件者若每天超過 5,000 封郵件，則必須強制設定完整 SPF、DKIM 與 DMARC 。 請參考以下完整的 google 官方說明

https://support.google.com/a/answer/81126?hl=zh-Hant

Yahoo 也同樣發布類似政策，從 2024 年第一季起，要求完整寄件網域 DNS 設定，請參考 Yahoo 官方說明

https://blog.postmaster.yahooinc.com/post/730172167494483968/more-secure-less-spam

11.1.2. 簡化取消訂閱

Google 的寄件者指南內容完整詳盡，最重要就是要設定本文所提到相對應 SPF/DKIM/DMARC，除此之外，並詳述其餘相關要求，特別是簡化取消訂閱。Google 跟 Yahoo 也都同時提到取消訂閱要能簡單執行，最好是”一鍵”就能取消。國際間已經制定相關通信協定，稱為"List-Unsubscribe"，Gmail 支援此郵件通訊協定，可以直接在收件者旁邊顯示取消訂閱連結，點擊就能直接取消。

但同樣為了防止被垃圾信業者所利用，寄件者網域信評需有一定等級(由 Google 自主認定)，Gmail 才會顯示此一”取消訂閱”字樣。

「沛盛資訊」所發出電子報，均支持”List-Unsubscribe”，在 Gmail 收到之後，收件人旁就能取消訂閱。

11.2.Google 郵件管理者工具

電子報發出後，到 Gmail、Yahoo Mail 等信箱，是否被放入垃圾信箱，有沒有被收件人檢舉垃圾信，這些是屬於收信服務器才會知道的指標，無法透過「沛盛資訊」報表得知。

Gmail 跟 Yahoo 都提供郵件管理員工具(Postmaster)，建議發送電子報品牌廠商一定要設定。以下說明，將以 Google 郵件管理員工具做詳細說明。

- Google 郵件管理員工具(Google Postmaster) https://www.gmail.com/postmaster/
- Yahoo 郵件管理員工具 (Sender Hub) https://senders.yahooinc.com/

但要看到完整的數據，前提是你每月發送到 Gmail 的郵件數量需要超過一定數量(由 Google 自主認定)，這是因為 Google 需要大量數據來進行分析。如果郵件數量不足，可能看不到完整的報表。

11.2.1. SPF、DKIM 和 DMARC 是否正確設定

Authentication 指標可顯示 SPF/DKIM/DMARC 是否正確。這些指標除了由 Gmail 原始檔可以查看之外，也可以透過此報表查看是否正確設定。

11.2.2. 寄件網域的信賴程度

表示寄件網域的信賴程度(reputation)。若為知名企業的寄件網域信賴度通常較高，一個剛設立不久的網域信賴程度低，報表中會顯示高、中、低的評級。

11.2.3. 寄件 IP 信賴程度

表示發送郵件的 IP 的信賴程度。使用沛盛資訊的發送郵件，由於有數量龐大發送 IP，IP 信賴程度會很高。

11.2.4. 寄件人郵件是否被檢舉

Spam Rate 也就是垃圾郵件率。這表示電子報被 Gmail 的收信人舉報為垃圾郵件的比例。即使你的郵件是合法發送的，收信人也有可能舉報，因此你的郵件一定要提供取消訂閱的選項，以降低被舉報的可能性。

11.2.5. 其餘指標

以上為比較重要指標，Postmaster 另有加密(Encryption) 指標，顯示郵件是否使用 TLS 加密。透過沛盛資訊發送的郵件都已使用 TLS 加密。

Delivery Errors 指標，表示郵件發送失敗的比率。正規的電子報發送者，這個比率應該極低，且可在電子報報表中查看。

Feedback Loop 指標，這是被使用者抱怨的綜合指標，通常需要額外設定在檔頭，多數寄件廠商可以不需做設定。

12. 網域設定示範

12.1.PCHOME DNS 設定

12.1.1. 管理 DNS 設定

登入 PChome 買網址後，到「管理我的網址」，再到想要設定之網域，選取「DNS 設定與修改」

12.1.2. 設定主網域郵件 DNS

主機檔案設定

主機 / 次網域 例: www 或 mail	地址	類型	優先權	轉址
www	[redacted]	A		
	[redacted]	A		
	[redacted]	A		
	[redacted]	MX	5	
	[redacted]	TXT(SPF)		
	v=spf1 include:spf.neweredm.com a mx ptr ?all	TXT(SPF)		
s1024._domain	k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GN	TXT(SPF)		
_dmarc	v=DMARC1; p=none	TXT(SPF)		

1. 實際填入數值

主機	地址	類型	說明
	v=spf1 include:spf.neweredm.com a mx ~all	TXT	SPF
s1024._domainkey	k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC5T4C4tyHsrVyiFZcqw4DGRDgfqtaPhEYqFSz/FSvVJywU1pBNF3rWkaaOjrzEIIb1vcIydgGi7xSXGbPqof9AnTHgVbX2cIASW09fTwTLokzj0dZ9gx9/Lsy7mjNvna4JQhLGl25oFsv2x3fwoRoynTw+2B9bRzCbTwtGX9mWOwIDAQAB;	TXT	DKIM (需同一行，不可斷行)
_dmarc	v=DMARC1; p=none	TXT	DMARC

2. 增加追蹤網址

若有需要設定點擊追蹤連結為自有網域名稱，請增加以下設定：

主機	地址	類型	說明
edm	hl.itpison.com	CNAME	點擊連結將為: edm.sample123.com

12.1.3. 設定在子網域

以上設定為使用原有網域(假設為 sample123.com)，若要設定在子網域，如 edm.sample123.com

主機	地址	類型	說明
edm	(原本的官網 IP)	A	建立子網域
edm	v=spf1 include:spf.neweredm.com a mx ~all	TXT	子網域 SPF
s1024._domainkey.edm	k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC5T4C4tyHsrVyiFZcqw4DGRDgfqtaPhEYqFSz/FSvVJywU1pBNF3rWkaaOjrzEIIb1vcIydgGi7xSXGbPqof9AnTHgVbX2cIASW09fTwTLokzj0dZ9gx9/Lsy7mjNvna4JQhLGl25oFsv2x3fwoRoynTw+2B9bRzCbTwtGX9mWOwIDAQAB;	TXT	子網域 DKIM (需同一行，不可斷行)
_dmarc.edm	v=DMARC1; p=none	TXT	子網域 DMARC

新增 MX 與點擊追蹤網域

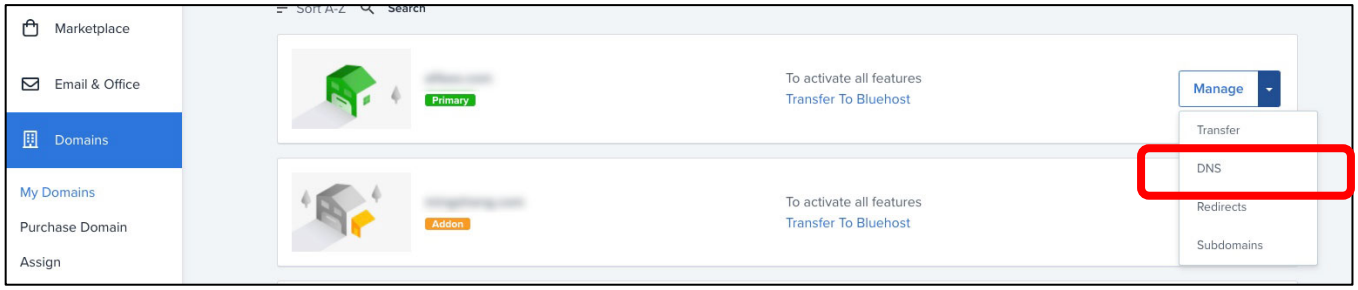
主機	地址	類型	優先	說明
edm	mx1.neweredm.com.(註)	MX	10	郵件收信
edm	mx2.neweredm.com.(註)	MX	10	郵件收信
edm	hl.itpison.com.(註)	CNAME		點擊連結將為: edm.sample123.com

註：PChome 的 DNS 設定，需要在 MX 與 CNAME 地址後面加個點 ‘.’

12.2.CPANEL 網域管理平台 DNS 設定

12.2.1. 管理 DNS 設定

cPanel 為國外流行之網域管理平台，進入平台之「Domain」為網域管理，之後選取「DNS」



12.2.2. 設定郵件 DNS

選取 TXT 類型後，依序填入本文建議之選項即可。
(註：下圖之 SPF，Host Record 為 @，代表原有之該網域。)