Bind DNSSEC 簽署教學(手動簽署)

本文說明如何利用 Bind 進行 DNSSEC 簽署，利用 Bind 既有的指令完成域名簽署。此簽署方式使用的指令參數較多，但適用於 Bind9 所有版本建議對 DNSSEC 與 DNS 運作原理有基本認知後再行操作會比較容易理解。

備註：本文使用 Bind 提供之 dnssec-signzone 指令進行簽署，此指令僅將既有的域名資料(Zone file)簽署，不會自動進行金鑰替換(Key Rollover)，建議了解簽署方式後自行修改域名資料維護流程，較不容易出錯。

建議對象：

了解 DNS 與 DNSSEC 運作流程，且熟悉 Bind 基本設定方式與操作。

使用環境：

Ubuntu Server 12.0.4（已安裝 Bind-9.9.3 Patch2）
Bind-9.9.3 Patch2

簽署環境：

以下簽署利用 Bind 做為權威主機，簽署的域名為 dnssec.dnssec-test.tw，Bind 之設定(named.conf)與域名資料(zone file)如下：

named.conf（節錄內容）

```
zone "dnssec.dnssec-test.tw" IN {
        type master;
        file "/tmp/test/hosts.dnssec.dnssec-test.tw";
};
```

hosts.dnssec.dnssec-test.tw

```
$TTL 3600
@       IN      SOA     dns.dnssec.dnssec-test.tw
hostmaster.dnssec-test.tw.  (
        2013082901          ; serial
        1D                  ; refresh
        30M                 ; retry
        1W                  ; expire
        1D )                ; minimum
 IN      NS      dns.dnssec.dnssec-test.tw.
dns         IN      A       192.168.1.1
www         IN      A       192.168.1.2
www2        IN      CNAME   www
```

DNSSEC 規劃：

在進行簽署前，務必先確定簽署時所會用到的參數設定如下：

- ZSK 加密演算法
- KSK 加密演算法
- ZSK 長度
- KSK 長度
- NSEC or NSEC3
- Key Rollover(ZSK,KSK)

此文件將以下列參數規格進行簽署：

ZSK 加密演算法	RSASHA256
KSK 加密演算法	RSASHA256
ZSK 長度	2048
KSK 長度	2048
NSEC or NSEC3	NSEC3
Key Rollover(ZSK,KSK)	ZSK: 1 個月, KSK: 暫無期限

DNSSEC 簽署：

DNSSEC 簽署主要分成三個步驟如下：

步驟(一)、生成驗證金鑰(ZSK, KSK)
步驟(二)、簽署域名與重啟
步驟(三)、後續維運

以下將針對此三個步驟說明。

步驟(一)、生成驗證金鑰(ZSK, KSK)

此章節將透過指令(dnssec-keygen)來產生簽署時所需金鑰(ZSK, KSK)。

生成 KSK 金鑰：

此步驟預計產生一把無期限之 KSK 金鑰於 /tmp/test/KSK 資料夾下，並用於簽署域名 dnssec.dnssec-test.tw 時使用。

產生 KSK
dnssec-keygen -r /dev/urandom -a RSASHA256 -f KSK -K /tmp/test/KSK -P now -A now -b 2048 -n ZONE dnssec.dnssec-test.tw

指令執行完成後，可於設定之資料夾(/tmp/test/KSK)下找到生成的兩個金鑰檔案：

- Kdnssec.dnssec-test.tw.+008+33004.key (KSK 公鑰)
- Kdnssec.dnssec-test.tw.+008+33004.private (KSK 私鑰)

至此已完成 KSK 金鑰的產生！

生成 ZSK 金鑰：

此步驟預計產生一把期限一個月之 ZSK 金鑰於 /tmp/test/ZSK 資料夾下，並用於簽署域名 dnssec.dnssec-test.tw 時使用。

產生 ZSK
dnssec-keygen -r /dev/urandom -a RSASHA256 -K /tmp/test/ZSK -P 20130725000000 -A 20130728000000 -I 20130902000000 -D 20130905000000 -b 2048 dnssec.dnssec-test.tw

指令執行完成後，可於設定之資料夾(/tmp/test/ZSK)下找到生成的兩個金鑰檔案：

- Kdnssec.dnssec-test.tw.+008+58509.key (ZSK 公鑰)
- Kdnssec.dnssec-test.tw.+008+58509.private (ZSK 私鑰)

其中可以注意到，這邊設定了四個時間參數分別為：

- Publish: 20130725000000 (Thu Jul 25 08:00:00 2013)
- Activate: 20130728000000 (Sun Jul 28 08:00:00 2013)
- Inactive: 20130902000000 (Mon Sep 2 08:00:00 2013)
- Delete: 20130905000000 (Thu Sep 5 08:00:00 2013)

至此已完成 ZSK 金鑰的產生！

步驟(二)、簽署域名與重啟

此章節將透過指令(dnssec-signzone)來簽署域名 dnssec.dnssec-test.tw 。

首先必須先將簽署時使用的公鑰放入網域名檔案中，以利查詢驗證使用。
為了讓後續域名資料易於維護，先將原始域名檔案
(hosts.dnssec.dnssec-test.tw)複製一份出來
(hosts.dnssec.dnssec-test.tw.dnssec)。

指令

cat hosts.dnssec.dnssec-test.tw > hosts.dnssec.dnssec-test.tw.dnssec

接著進行把公鑰放入網域名稱資料(hosts.dnssec.dnssec-test.tw.dnssec)中。

指令(KSK 公鑰)
cat KSK/Kdnssec.dnssec-test.tw.+008+33004.key >> hosts.dnssec.dnssec-test.tw.dnssec
備註： 請注意執行指令時的路徑位置，並自行調整檔案路徑，避免無法找到對應檔案之情況！

指令(ZSK 公鑰)
cat ZSK/Kdnssec.dnssec-test.tw.+008+58509.key >> hosts.dnssec.dnssec-test.tw.dnssec
備註： 請注意執行指令時的路徑位置，並自行調整檔案路徑，避免無法找到對應檔案之情況！

最後便可以進行簽署域名資料的步驟。另外在簽署時會需要指定生成的簽章有效時間，這邊習慣性會設定成與 ZSK 的 Active 與 Inactive 時間相同，當然也可以自行設定。此處會簽署域名檔案(hosts.dnssec.dnssec-test.tw.dnssec)，簽署完成後會產生簽署後的域名檔案
(hosts.dnssec.dnssec-test.tw.dnssec.signed)。

簽署域名指令
dnssec-signzone -3 123456 -o dnssec.dnssec-test.tw -s 20130728000000 -e 20130902000000 -k KSK/Kdnssec.dnssec-test.tw.+008+33004.key ./hosts.dnssec.dnssec-test.tw.dnssec ./ZSK/Kdnssec.dnssec-test.tw.+008+58509.key
備註： 指令僅提供參考用，因環境不同，實際簽署指令請依簽署時的路徑與環境來設定。

執行完成後，已將域名資料簽署完成，並且產生兩個額外的檔案：

- dsset-dnssec.dnssec-test.tw. (DS 檔案，用於遞交上層驗證使用)
- hosts.dnssec.dnssec-test.tw.dnssec.signed (含有簽署資料之域名檔案)

因簽署後僅是將原本的域名資料簽署完成，Bind 尚未將簽署後的結果讀進記憶體中，故重新將設定檔案修改讓 Bind 讀取簽署後的資料。

named.conf（節錄內容，修改檔案內容讓簽署的資料能讀取到）

```
zone "dnssec.dnssec-test.tw" IN {
        type master;
        file "/tmp/test/hosts.dnssec.dnssec-test.tw.dnssec.signed";
};
```

最後重新啟動 Bind 後，若啟動正常即表示簽署成功，確認先前設定的域名資料都有被正確的簽署後，即可進行 DS 向上層註冊的動作，完成整個 DNSSEC 的設定。

指令(重新啟動 Bind)

```
rndc reload
```

步驟(三)、後續維運

若在已簽署完成的權威主機上，後續碰到需要修改域名資料的狀況可透過下列步驟修改：

1. 修改域名資料(hosts.dnssec.dnssec-test.tw)

hosts.dnssec.dnssec-test.tw

```
$TTL 3600
@       IN      SOA     dns.dnssec.dnssec-test.tw
hostmaster.dnssec-test.tw.  (
        2013082901          ; serial
        2013082902          ; serial
        1D                  ; refresh
        30M                 ; retry
        1W                  ; expire
        1D )                ; minimum
 IN      NS      dns.dnssec.dnssec-test.tw.
dns         IN      A       192.168.1.1
dns         IN      A       192.168.11.11
www         IN      A       192.168.1.2
www2        IN      CNAME   www
```

2. 複製域名資料(hosts.dnssec.dnssec-test.tw ->

hosts.dnssec.dnssec-test.tw)
為了讓後續域名資料易於維護，先將原始域名檔案
(hosts.dnssec.dnssec-test.tw)複製一份出來
(hosts.dnssec.dnssec-test.tw.dnssec)。

指令
cat hosts.dnssec.dnssec-test.tw > hosts.dnssec.dnssec-test.tw.dnssec

3. 公鑰放入網域名稱資料(hosts.dnssec.dnssec-test.tw.dnssec)
接著進行把公鑰放入網域名稱資料(hosts.dnssec.dnssec-test.tw.dnssec)中。

指令(KSK 公鑰)
cat KSK/Kdnssec.dnssec-test.tw.+008+33004.key >> hosts.dnssec.dnssec-test.tw.dnssec
備註： 請注意執行指令時的路徑位置，並自行調整檔案路徑，避免無法找到對應檔案之情況！

指令(ZSK 公鑰)
cat ZSK/Kdnssec.dnssec-test.tw.+008+58509.key >> hosts.dnssec.dnssec-test.tw.dnssec
備註： 請注意執行指令時的路徑位置，並自行調整檔案路徑，避免無法找到對應檔案之情況！

4. 簽署更新後的域名資料

簽署域名指令
dnssec-signzone -3 123456 -o dnssec.dnssec-test.tw -s 20130728000000 -e 20130902000000 -k KSK/Kdnssec.dnssec-test.tw.+008+33004.key ./hosts.dnssec.dnssec-test.tw.dnssec ./ZSK/Kdnssec.dnssec-test.tw.+008+58509.key
備註： 指令僅提供參考用,因環境不同,實際簽署指令請依簽署時的路徑與環境來設定。

5. 重啟 Bind

指令(重新啟動 Bind)
rndc reload