Bind DNSSEC 簽署教學(自動簽署)

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。此簽署方式使用的方式為 Bind9.9.x 以後之版本適用，透過 Bind9.9.x 後的版本提供 inline-signing 之方式，來完成自動簽署的動作。
備註：使用自動簽署的方式操作上較為容易，也僅需將欲使用的金鑰(ZSK, KSK)預先產生好即可，但因透過 Bind 自動化簽署的機制，較難掌握簽署的流程與細節(因為 Bind 自動做掉了)。

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 dnssec2.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 "dnssec2.dnssec-test.tw" IN {
        type master;
        key-directory "/tmp/test/dnskey";
        auto-dnssec maintain;
        inline-signing yes;
        file "/tmp/test/hosts.dnssec2.dnssec-test.tw";
};
```

hosts.dnssec.dnssec-test.tw

```
$TTL 3600
@       IN      SOA     dns.dnssec2.dnssec-test.tw
hostmaster.dnssec-test.tw.  (
        2013082901          ; serial
        1D                  ; refresh
        30M                 ; retry
        1W                  ; expire
        1D )                ; minimum
 IN      NS      dns.dnssec2.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/dnskey 資料夾下，並用於簽署域名 dnssec2.dnssec-test.tw 時使用。

產生 KSK
dnssec-keygen -r /dev/urandom -a RSASHA256 -f KSK -K /tmp/test/dnskey

-P now -A now -b 2048 -n ZONE dnssec2.dnssec-test.tw

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

- Kdnssec2.dnssec-test.tw.+008+33004.key (KSK 公鑰)
- Kdnssec2.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/dnskey 資料夾下，並用於簽署域名 dnssec2.dnssec-test.tw 時使用。

產生 ZSK
dnssec-keygen -r /dev/urandom -a RSASHA256 -K /tmp/test/dnskey -P 20130725000000 -A 20130728000000 -I 20130902000000 -D 20130905000000 -b 2048 dnssec2.dnssec-test.tw

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

- Kdnssec2.dnssec-test.tw.+008+58509.key (ZSK 公鑰)
- Kdnssec2.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 rndc 指令來簽署域名 dnssec2.dnssec-test.tw 。
因為是透過 Bind 的 inline-signing 方式來簽署 DNSSEC，所以需要做的動作很單純只需要啟動 Bind，Bind 就會自動到放置金鑰的資料夾(/tmp/test/dnskey)去抓取要用的金鑰來簽署。

指令
rndc reload dnssec2.dnssec-test.tw

重新啟動後，會發現原本放置域名資料夾下多出三個檔案：

- hosts.dnssec2.dnssec-test.tw.jbk
- hosts.dnssec2.dnssec-test.tw.signed
- hosts.dnssec2.dnssec-test.tw.signed.jnl

此為自動簽署時會使用的檔案，不用理會即可。

因為 Bind 預設會使用 NSEC 來簽署，若本來就欲使用 NSEC 來簽署，至此已經完成域名的簽署了。若是要使用 NSEC3 來簽署的話，則必須多執行 rndc signing 指令來進行簽署，如下：

指令
rndc signing -nsec3param 1 0 10 123321 dnssec2.dnssec-test.tw

至此已經完成 NSEC3 簽署的步驟，整個域名 DNSSEC 簽署也已經完成。
確認域名簽署結果正確後，即可進行遞交 DS 之作業，在自動化簽署的方式下，要取得 DS 的方式可透過下列指令取得：

指令
/app/bind991p3/sbin/dnssec-dsfromkey /tmp/test/dnskey/ Kdnssec2.dnssec-test.tw.+008+33004.key
備註： Kdnssec2.dnssec-test.tw.+008+33004.key 為 KSK 之金鑰，因為 DS 資料主要透過 KSK 產生，故需要指定 KSK 公鑰的位置。

執行結果
dnssec2.dnssec-test.tw. IN DS 33004 8 1 56DE940A1AED70A8D4B951E63517EA613E028455 dnssec2.dnssec-test.tw. IN DS 33004 8 2 CC66E4DC9679479CDC5E443493FCCDA2C8862662D73C05F70E9E575E 39E0E862

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.dnssec2.dnssec-test.tw)

hosts.dnssec2.dnssec-test.tw
$TTL 3600 @ IN SOA dns.dnssec2.dnssec-test.tw hostmaster.dnssec-test.tw. (

```
        2013082901          ; serial
        2013082902          ; serial
        1D                  ; refresh
        30M                 ; retry
        1W                  ; expire
        1D )                ; minimum
 IN      NS      dns.dnssec2.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. 簽署更新後的域名資料

指令
rndc signing -nsec3param 1 0 10 123321 dnssec2.dnssec-test.tw

至此 Bind 便會自動將修改的內容更新完成。