

# DNSSEC během 6 minut

- Historie aktualizací

- Nečíslovaná – Původní vydání

- 1.1 – Úpravy gramatiky, přidáno číslo verze

- 1.2 – Rozdělení na 2 části

- 1.3 – Oprava v dnssec-keygen, přidána historie aktualizací

- 1.4 – Oprava DLV

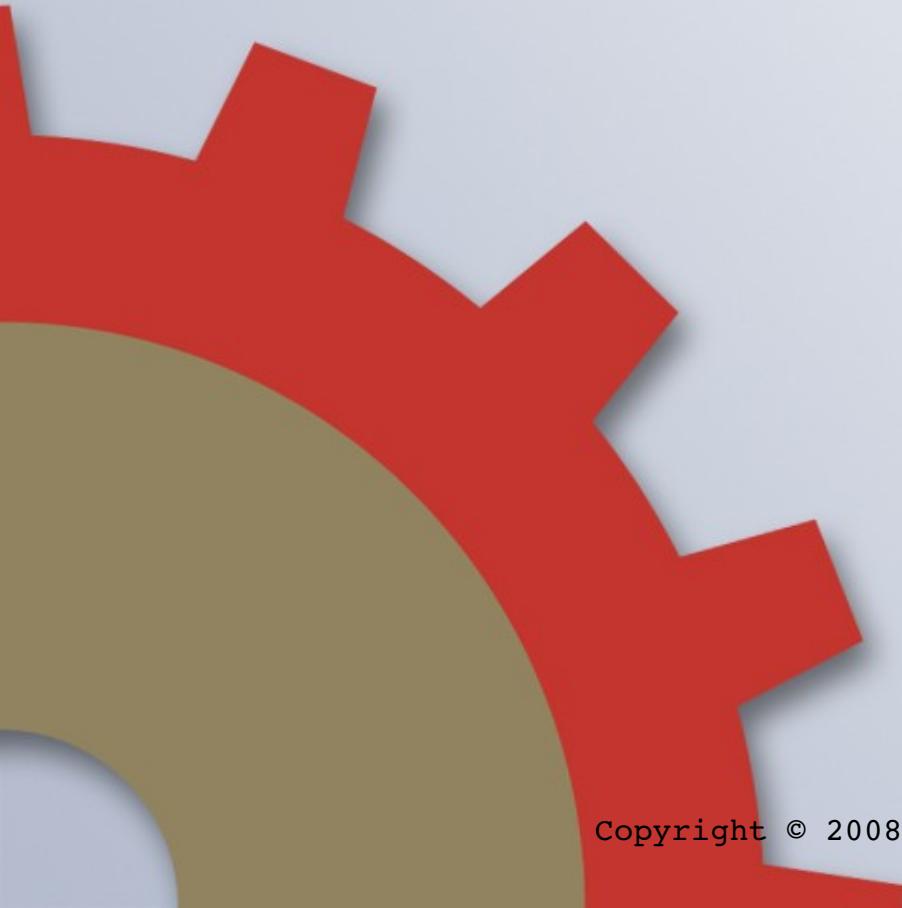
- 1.5 – Vyčištění rozdělení a aktualizace udp53.org

- základní linie verze pro čínský překlad

# Díky...

- Francis DuPont
- Mark Andrews
- Tim Brown
- Håvard Eidnes
- Bruce Esquibel
- Carl Byington
- 孙国念 (SUN Guonian)

# DNSSEC během 6 minut



Alan Clegg

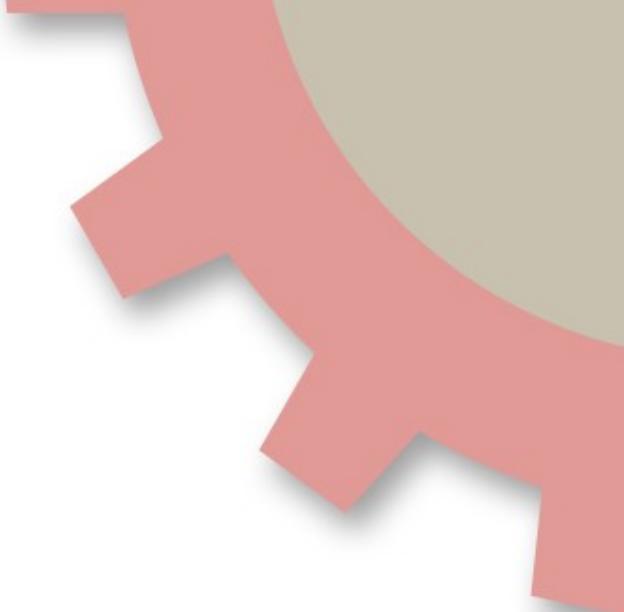
Programátor  
oddělení podpory

Internet Systems Consortium

[alan\\_clegg@isc.org](mailto:alan_clegg@isc.org)

Verze 1.5





# Objasnění DNSSEC

# Objasnění DNSSEC

- DNSSEC umožňuje autoritativním serverům poskytovat k „standardním“ DNS datům navíc digitální podpisy RRsetů
- Resolvery ověřující DNSSEC podpisy (dále „validující resolvery“) poskytují potvrzené odpovědi s prokázanou integritou

# Objasnění DNSSEC

- Klienti, kteří používají validující resolvency, získávají garantovaná „správná“ data
  - s určitou úrovní „garance“
- Odpovědi, které nejsou validní, jsou klientovi vráceny z nadřazeného resolveru s chybou „SERVFAIL“

# Nasazení DNSSECu



# Nasazení DNSSECu

- Jednorázové aktivity:
  - Ujasněte si adresářovou strukturu na autoritativním serveru a pojmenování zónového souboru
  - Povolte DNSSEC na autoritativních serverech
  - Povolte DNSSEC na rekurzivních serverech

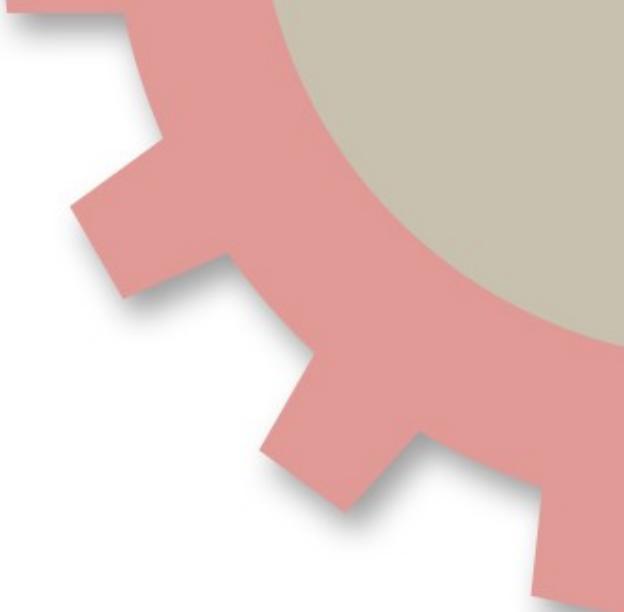
# Nasazení DNSSECu

- Povolte DNSSEC pro každou zónu
  - Vygenerujte ZSK a KSK
  - Připojte klíče do zónového souboru
  - Podepište zónu
  - Změňte odkaz na zónový soubor v named.conf na podepsaný zónový soubor
  - Znovu načtěte zónu

# Nasazení DNSSECu

- Umístěte DS záznamy do nadřazené zóny
- V případě, že nadřazená zóna nepoužívá DNSSEC, umístěte DLV záznamy do DLV registru





# Všechny tyto kroky... podrobně!

# Připravte adresářovou strukturu

- K dispozici jsou nástroje, jež usnadňují údržbu zóny, ale nejlépe pracují se standardizovanou adresářovou strukturou
- Umístěte všechny soubory zóny do jediného adresáře

# Povolte DNSSEC na autoritatívnych serverech

```
options {  
    dnssec-enable yes;  
};
```

- Vyžaduje BIND s podporou SSL a nainstalované OpenSSL knihovny

# Povolte DNSSEC na rekurzivních serverech

```
options {  
    dnssec-enable yes;  
    dnssec-validation yes;  
};
```

- Validace se provádí na rekurzivních, nikoli na autoritativních serverech.



# Zabezpečení zóny

- Pro každou zónu jsou vytvořeny dva klíče
  - ۚ ۱) Klíč podepisující zóny (ZSK) – používá se k podpisu dat v zóně
  - ۚ ۲) Klíč podepisující klíče (KSK) – používá se k podpisu klíče podepisujícího zóny a k vytvoření „důvěryhodného vstupního bodu (SEP)“ pro zónu



# Vytvořte klíče

- Vytvoření ZSK

```
dnssec-keygen -a RSASHA1 -b 1024  
-n ZONE zonename
```

- Využívá algoritmus RSA SHA1
- o délce 1024 bitů
- Toto je DNSSEC klíč pro zónu (-n ZONE)



# Vytvořte klíče

- Vytvoření ZSK

```
dnssec-keygen -a RSASHA1 -b 1024  
-n ZONE zonename
```

- Vytvoří 2 soubory

Kzonename+<alg>+<fing>.key

Kzonename+<alg>+<fing>.private

- .key je veřejnou částí klíče, .private je soukromou částí klíče



# Vytvořte klíče

- Vytvoření KSK

```
dnssec-keygen -a RSASHA1 -b 4096  
-n ZONE -f KSK zonename
```

- Využívá algoritmus RSA SHA1
- o délce 4096 bitů
  - Takto velký klíč potřebuje velkou entropii!
- Toto je DNSSEC klíč pro zónu (-n ZONE)
- Má nastavení bitu (KSK) důvěryhodného vstupního bodu



# Připravte zónu

- Přidejte veřejné části obou KSK a ZSK k zóně, která má být podepsána

Direktiva \$INCLUDE v zonefile nebo  
cat Kzonename+\*.key >> zonefile

- Dejte si pozor, abyste nepoužili pouze jednu „>“! (přepíše soubor)



# Podepište zónu

- Přidejte RRSIG, NSEC a přiřazené záznamy k zóně  

```
dnssec-signzone [-o zonename]
                  [-N INCREMENT] [-k KSKfile]
                  zonefile [ZSKfile]
```
- Název zóny (`zonename`) je implicitně název souboru (`zonefile`)
  - Pojmenujte soubor podle zóny!



# Podepište zónu

```
dnssec-signzone [ -o zonename ]  
[ -N INCREMENT ] [ -k KSKfile ]  
zonefile [ ZSKfile ]
```

-N INCREMENT automaticky inkrementuje  
sériové číslo během podepisování

- Odstraňuje chybu způsobenou „lidským faktorem“



# Podepište zónu

```
dnssec-signzone [ -o zonename ]  
[ -N INCREMENT ] [ -k KSKfile ]  
zonefile [ ZSKfile ]
```

- KSKfile je implicitně Kzonefile\*
  - s nastavením bitu SEP
- ZSKfile je implicitně Kzonefile\*
  - bez nastavení bitu SEP



# Podepište zónu

```
dnssec-signzone [ -o zonename ]  
[ -N INCREMENT ] [ -k KSKfile ]  
zonefile [ ZSKfile ]
```

Výstupní soubor je `zonefile.signed`

- Seřazený podle abecedy
- včetně RRSIG, NSEC & DNSKEY RR
- Mnohem větší než předtím!



# Aktualizujte named.conf

Nahradíte

```
zone "zonename" {  
    file "dir/zonefile";  
};
```

Za

```
zone "zonename" {  
    file "dir/zonefile.signed";  
};
```



# Začněte poskytovat podepsanou zónu

- Načtěte znova konfiguraci named

```
rndc reconfig
```

```
rndc flush
```

- Nyní poskytujete DNSSEC podepsané zóny



# Problematika pravidelné údržby

# Pravidelná údržba zóny

- Podpisy mají životnost
  - Datum „vzniku“ – 1 hodina před spuštěním dnssec-signzone
  - Datum expirace – 30 dní po spuštění dnssec-signzone
- Expirované podpisy způsobí, že zóna nepůjde ověřit!

# Pravidelná údržba zóny

- Pokaždé, když upravíte zónu – nebo minimálně každých 30 dnů (mínus TTL) musíte znova spustit dnssec-signzone
- Pokud to neuděláte
  - ↳ Data zóny budou zastaralá
  - ↳ Data zóny budou „ZTRACENA“

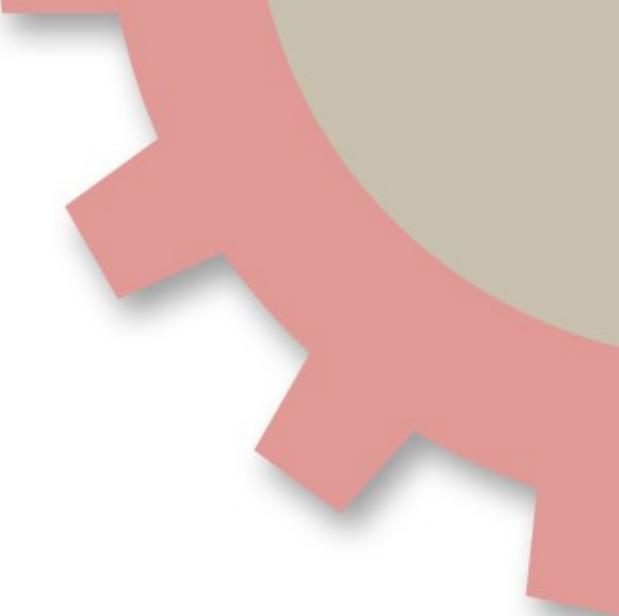
# Pravidelná údržba klíče

- Klíče je zapotřebí střídat
  - Nemají „datum expirace“
- Čím déle je klíč veřejně viditelný, tím větší je pravděpodobnost, že bude prolomen
- Prolomení (zcizení) klíče může vést k potřebě „výměny“ klíče

# Pravidelná údržba klíčů

- KSK by měl být vyměněn jednou ročně
- ZSK by měl být vyměněn každé 3 měsíce
- Postup je mnohem složitější, než ukazuje tato prezentace
- Jsou dostupné automatické nástroje





# Reálný příklad

# Příklad s pravými jmény

- zonename k podpisu je `udp53.org`
- jméno zonefile je `udp53.org`
- Adresář obsahující zonefile je  
`/zone/udp53.org`

Úplná cesta k zonefile je:

`/zone/udp53.org/udp53.org`



# Příklad s pravými jmény

```
<přidejte dnssec-enable k named.conf>  
cd /zone/udp53.org  
dnssec-keygen -a rsashal -b 1024 -n ZONE  
    udp53.org  
  
dnssec-keygen -a rsashal -b 4096 -n ZONE  
    -f KSK udp53.org  
  
cat Kudp53*key >> udp53.org  
  
dnssec-signzone -N INCREMENT udp53.org  
<změňte vstupy zónového souboru pro použití  
.signed>
```



# Příklad s pravými jmény

- Původně, /zone/udp53.org obsahovala POUZE zonefile "udp53.org"
- Po skončení:
  - 2 zSK soubory (.key a .private)
  - 2 KSK soubory (.key a .private)
  - 2 zónové soubory (nepodepsané a .signed)
  - soubor dsset-udp53.org (DS RRs)
  - soubor keyset-udp53.org (DNSKEY RRs)

# Příklad s pravými jmény

- zonefile začal s
  - 71 řádky
  - 2 378 znaky
- Skončil s
  - 665 řádky
  - 26 970 znaky



# Oznamte nadřazené zóně DNSSEC

- Vaše nadřazená zóna musí nyní vložit "DS" RR pro vytvoření řetězu důvěry
- Postupy se budou lišit podle organizací, ale musí být provedeny bezpečně
  - bude vyžadovat použití dsset- a/nebo keyset- souborů

# Nadřazená zóna bez podpory DNSSECu

- Ne všechny TLD podporují DNSSEC
  - Ve skutečnosti podporuje v současnosti DNSSEC **VELMI MÁLO** TLD
- Poskytněte váš DNSKEY těm stranám, u kterých chcete, aby ověřovali vaši zónu.
  - Musí to být provedeno bezpečně, nejen pouze jako "dig"

# Pevné body důvěry (Trust Anchors)

# Pevné body důvěry

- Pro ověření ostatních zón musíte vložit „pevný bod důvěry“ pro každý zónu, kterou budete chtít ověřovat
- Nejvyšší pevný bod důvěry bude pocházet od podepsané root zóny (“.”)

# Pevné body důvěry

- Až bude podepsána root zóna, bude vyžadován pouze jeden pevný bod důvěry
- Dokonce i poté, co bude podepsána root zóna, je stále možné a pravděpodobné, že bude potřeba mít další pevné body důvěry

# Pevné body důvěry

- V současnosti (Léto 2008), root zóna (“.”) není podepsána
- Jsou vyžadovány jednotlivé pevné body důvěry
- Pevné body důvěry musí být získány důvěryhodnými prostředky
- DNS není jedním z těchto prostředků, AVŠAK...



# Pevné body důvěry

```
dig udp53.org DNSKEY
```

```
udp53.org. 14400 IN DNSKEY 256 3 5 BE[...]/v1
```

```
udp53.org. 14400 IN DNSKEY 257 3 5 BE[...]lylot7
```

- Pomocí digu získáme DNSSEC klíče, které mohou být ověřeny pomocí dalších prostředků (web, telefon, tištěná média, atd.)

# Pevné body důvěry

- bude zapotřebí, aby `named.conf` obsahoval:

```
trusted-keys {  
    "udp53.org." 257 3 5 "BE[...]1ylot7";  
    "isc.org." 257 3 5 "BEAAAAO[...]ZCqoif";  
};
```

- Klíč pro KAŽDOU zónu, kterou chcete ověřovat

# Pevné body důvěry

- Správa jednotlivých pevných bodů důvěry je složitá
- Aby pomohlo vyřešit tento problém, vytvořilo ISC DLV "Domain Lookaside Validation" RR záznam koncept DLV registru



# Domain Lookaside Validation



# DLV

- Při ověřování hledá resolver v nadřazené zóně záznam DS pro zónu, která je ověřována
- Pokud neexistuje, je vytvořen dotaz na záznam DLV v zóně registru DLV
- Pokud je úspěšná, je DLV RR použito jako DS pro danou zónu

# Příklad DLV

- `udp53.org` je podepsaná
- Vlastník `udp53.org` se registroval do DLV registru u ISC
- Je vytvořen DNSSEC dotaz na A RR jména `www.udp53.org`
- Není nalezen DS záznam v `.org` pro zónu `udp53.org`

# Příklad DLV

- Resolver bez zapnutého DLV nebude v tomto bodě schopen provést ověření
- Resolver se zapnutým DLV bude hledat `udp53.org.dlv.isc.org.` DLV RR
- Tento DLV RR pak bude použit jako DS pro zónu `udp53.org.`



# Povolení DLV

- Použití DLV pro ověření je provedeno na rekurzivním serveru
  - Pro DLV registr musí být vytvořen důvěryhodný klíč
  - Konfigurace dnssec-lookaside musí být napojena na DLV trust anchor

# Povolení DLV

- named.conf:

```
trusted-keys {  
    dlv.isc.org. 257 3 5  
    "BEA[...]uDB";  
};  
  
options {  
    dnssec-lookaside ".";  
    trust-anchor dlv.isc.org.;  
};
```



# Generování DLV RRs

- Při podepisování zóny pro registrátora DLV přidejte přepínač “-l” (malé L) k dnssec-signzone:  
`dnssec-signzone [-o zonename] [-N INCREMENT] -l dlvzone [-k KSKfile] zonefile [ZSKfile]`
- dlvzone bude závislá na DLV registru

# Generování DLV RRS

- Na základě předchozího příkladu:  
dnssec-signzone -N INCREMENT  
-l **dlv.isc.org.** udp53.org
- V tomto bodě bude vytvořen soubor  
dlvkey-udp53.org, který je  
rovnou připraven k odeslání správci  
ISC DLV



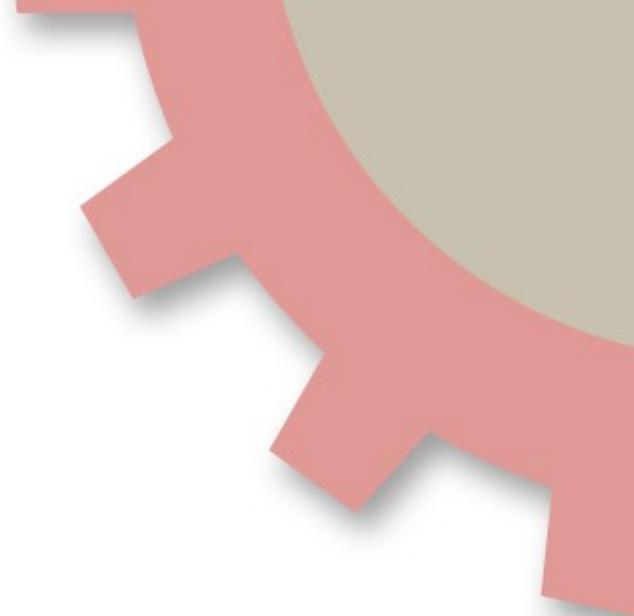
# Registrace v DLV

- Kontaktujte registrátoru DLV pro instrukce jak prokázat vlastnictví zóny a platnost DLV RR záznamu
- Vložení vašeho DLV RR záznamu do registru DLV musí být provedeno důvěryhodným způsobem

# ISC registr DLV

<http://www.isc.org/ops/dlv/>





# Dotazy?

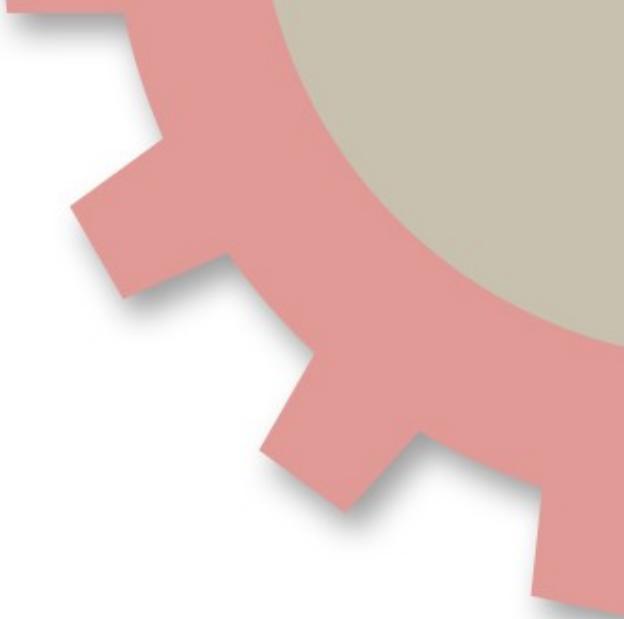
# Komentáře?



**Ne! Ne, ne, ne 6!**

Řekl jsem 7  
Nikdo to  
nezvládne za 6  
minut

Kdo nasadí  
DNSSEC během 6  
minut?



# Testování a ladění DNSSECu

# Testování DNSSECu

- Nyní, když distribuujete podepsané DNSSEC RR záznamy, funguje to?
- Mark Andrews uvedl, že DNSSEC může být laděn pouze pomocí příkazů “dig” a “date”
- Tady je jak na to!

# Dotazování na DNSSEC

- Dotaz vyžadující ověřená data z jakéhokoliv resolveru poskytne RRset v odpovědi
- Dotaz vyžadující nepodepsaná data z jakéhokoliv resolveru poskytne RRset v odpovědi

# Dotazování na DNSSEC

- Dotaz, který validujícímu resolveru vrátí upravená nebo neplatná data, skončí s chybou SERVFAIL
- Pro aplikace (a uživatele) se bude doména jevit jako „neexistující“
- Příznak CD v hlavičce umožní, aby i neplatná data byla odeslána

# výstup dig – bez DNSSECu

dig

```
; ; [ .. ] status: NOERROR
; ; flags: qr rd ra;
```

- Správná odpověď; odpověď (qr), požadovaná rekurze (rd), rekurze k dispozici (ra)

# výstup dig – bez DNSSECu

```
dig www.udp53.org a
```

```
; ; [..] status: NOERROR
```

```
; ; flags: qr rd ra;
```

- Z validujícího resolveru – tohle jsou garantovaná správná data



# výstup dig – bez DNSSECu

```
dig www.udp53.org a
```

```
; ; [..] status: NOERROR
```

```
; ; flags: qr rd ra;
```

- Ale jak víte, že váš resolver provádí validaci?

# výstup dig – s DNSSECem

```
dig +dnssec www.udp53.org a
```

```
; ; [..] status: NOERROR
```

```
; ; flags: qr rd ra ad
```

- Jako předtím, ale tentokrát autentizované!

# Dotazování na DNSSEC

- Pro vrácení příznaku **AD** musí mít resolver provádějící ověření pevný bod důvěry, který může být zpětně vystopován (pomocí DS RR záznamů)
- Pokud řetěz důvěry nevede k pevnému bodu důvěry, nebude příznak AD nastaven, ale RRSIG záznamy budou i tak vráceny

# výstup dig – DNSSEC

dig +dnssec [www.udp53.org](http://www.udp53.org) a

www.udp53.org. 3600 IN A 192.168.154.2

www.udp53.org. 3600 IN RRSIG A 5 3 3600 20080627122225  
20080617122225 46704 udp53.org.

XEkXkv9MCRiGbxO9T0dkNY+3y5EZRB6s6YOk0pFAVUL/y8VDeJphc8yb  
K6E/YLvraItdGvIvpy4P1OuIY09BGQ==

- Pokud je AD nastaveno, resolver má pevný bod důvěry, pokud ne, pořád máme data, která můžeme ověřit sami

# Dotazování na DNSSEC

- Pokud víme, že komunikujeme s validujícím resolverem a dostaneme zpět SERVFAIL, může se jednat o neověřená podepsaná data
- Pokud je to tak, nastavení bitu “CD” v dotazu způsobí, že resolver i tak zašle „nevalidní“ data

# výstup dig - DNSSEC

```
dig +dnssec +cd www.udp53.org a
```

```
www.udp53.org. 3600 IN A      192.168.154.2
```

```
www.udp53.org. 3600 IN RRSIG A 5 3 3600 20080627122225  
20080617122225 46704 udp53.org. xxxxxxxxxx
```

- Neplatný záznam RRSIG  
**(xxxxxxxxxx)**, ale s příznakem **+cd**,  
proto dostaneme odpověď



# výstup dig - DNSSEC

dig +dnssec +cd [www.udp53.org](http://www.udp53.org) a

www.udp53.org. 3600 IN A 192.168.154.2

www.udp53.org. 3600 IN RRSIG A 5 3 3600 **20030627122225**

**20030617122225** 46704 udp53.org.

XEkXkv9MCRiGbxO9T0dkNY+3y5EZRB6s6YOk0pFAVUL/y8VDeJphc8yb  
K6E/YLvraItdGvIvpy4P1OuIY09BGQ==

- Data v podpisu ukazují, že podpis je expirovaný
- Porovnejte s aktuálním datem



# Dotazování na DNSSEC

- Všimněte si, že je snadné zkontolovat datum na podpisech
- Je mnohem těžší (není v lidských silách?) najít chybu v klíči samotném
- Předchozí příklad je krajně nepřirozený (xxx?)

# Dotazování na DNSSEC

- Další problém, který může nastat je chybějící nebo jiný hash nebo klíč
  - DS v nadřazené zóně
  - DNSKEY v aktuální zóně
- Není těžké určit ani tuto chybu!

# výstup dig – DNSSEC

```
dig +dnssec +cd www.udp53.org
```

```
www.udp53.org. 3600 IN A      192.168.154.2
```

```
www.udp53.org. 3600 IN RRSIG A 5 3 3600 20080627122225
```

```
20080617122225 46704 udp53.org.
```

```
XEkXkv9MCRiGbxO9T0dkNY+3y5EZRB6s6YOk0pFAVUL/y8VDeJphc8yb  
K6E/YLvraItdGvIvpy4P1OuIY09BGQ==
```

- Podpis byl vytvořen s klíčem 46704

# výstup dig – DNSSEC

```
dig +cd +multi udp53.org dnskey
```

```
udp53.org. 14400 IN DNSKEY 256 3 5 (
BEAAAAO2oQi7U9m9i495S/XoAk+j8QxxnBHOn6fa7n1N
7xoqrSr/xzy3+IerFS1KgJz1gJGbTsGV0WI1/bvAzIEK
Uh+p ) ; key id = 46704
```

DNSKEY v zóně existuje

- Pokud ne, nepůjde ověřit!

# výstup dig – DNSSEC

```
dig +cd +multi udp53.org dnskey
```

```
udp53.org. 14400 IN DNSKEY 256 3 5 (  
    B[...]p ) ; key id = 46704
```

```
udp53.org. 14400 IN DNSKEY 257 3 5 (  
    B[...]J ) ; key id = 64249
```

- ZSK DNSKEY v zóně existuje
- Připojený KSK je 64249



# výstup dig – DNSSEC

```
dig +norec @gTLD udp53.org ds
```

```
; ; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29385  
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 2
```

- DS v nadřazené zóně neexistuje
- Pokud neuděláme DLV, tohle je důvod, proč se neautentizuje

# výstup dig – DNSSEC

```
dig +norec @gTLD udp53.org ds
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29385
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 2, ADDITIONAL: 2
```

- Server bude vracet odpovědi, ale bez příznaku „AD“
- Neexistuje řetěz důvěry až k pevnému bodu důvěry



# výstup dig – DNSSEC

```
dig udp53.org.dlv.isc.org dlv
```

```
udp53.org.dlv.isc.org. 3257 IN DLV 64249 5 2 (  
59C58FD329F1C33628C92FC4B763EF9ADB833804D60D  
18D439AB04F6302C20FD )
```

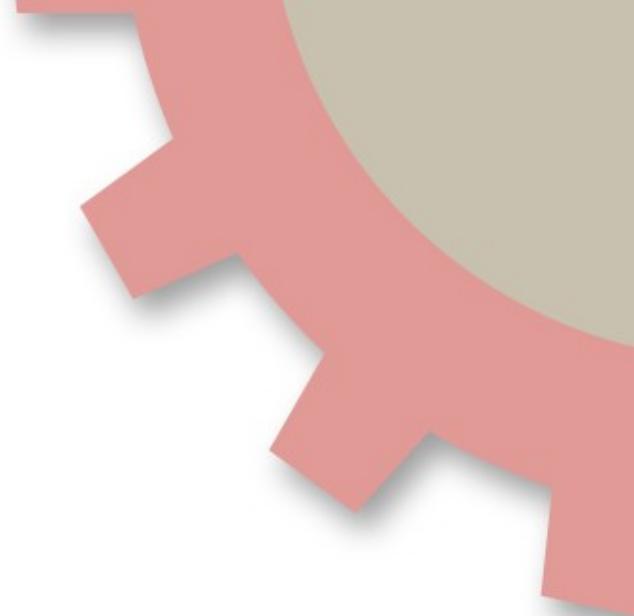
```
udp53.org.dlv.isc.org. 3257 IN DLV 64249 5 1 (  
D5D722703D848E85D85E8A8442AF47512B385418 )
```

- KSK 64249 DLV v registru ISC existuje, poskytuje DS pro zónu

# Řetěz důvěry

- Trust anchor pro `dlv.isc.org`
- DLV záznam pro  
`udp53.org.dlv.isc.org`
- KSK pro `udp53.org`
- ZSK pro `udp53.org`
- Podpis pro `www.udp53.org`
- bit AD nastaveno!





# Dotazy?

# Komentáře?