WORKSHOP GARR 2025

NET MAKERS

Attivazione di DNSSEC su nomi a dominio .it e .eu registrati con GARR

Marco Gallo

GARR

DNSSEC: 🔒 sicurezza per i Domini (.it e .eu) registrati con GARR

- Da Luglio 2025, GARR è tra i registrars accreditati per la gestione di domini con il protocollo di sicurezza DNSSEC
  - Panoramica su DNSSEC
  - Come richiedere l’attivazione di DNSSEC su domini di secondo livello .it e .eu

Perché attivare DNSSEC? (1)

- Il **DNS** è fondamentalmente un **protocollo non sicuro**
- Progettato negli anni '80 con la priorità di garantire la funzionalità e la velocità, non la sicurezza
- Opera sul principio della fiducia implicita: il server che interroga (resolver) accetta come vera la prima risposta che riceve
- **Non include** alcuna **prova crittografica** che sia stata inviata dal server autoritativo legittimo.

Perché attivare DNSSEC? (2)

- DNSSEC è stato introdotto per aggiungere un livello di **autenticità e integrità dei dati** alle risposte del DNS

  - E’ efficace contro qualsiasi attacco che comprometta l'integrità e l'autenticità dei dati DNS durante il transito o nel corso del processo ricorsivo di risoluzione

  - Garantisce che i dati provengono dal vero responsabile del dominio

Principali attacchi da cui DNSSEC offre protezione

- **DNS Spoofing**: un attaccante intercetta una richiesta DNS e risponde con un indirizzo IP falso prima che il nameserver autoritativo possa rispondere. L'obiettivo è reindirizzare l'utente verso altre destinazioni, ad esempio un sito web malevolo che può sembrare identico a quello legittimo

- **Cache Poisoning**: è una forma di spoofing in cui i dati falsi vengono inseriti nella cache di un resolver DNS. Una volta "avvelenata" la cache, tutti gli utenti che utilizzano quel resolver saranno reindirizzati al sito falso per un periodo di tempo prolungato

    - **Negazione Non Autenticata dell'Esistenza di un fqdn**: senza DNSSEC, un attaccante può far credere che un dominio esistente non esista. L'aggressore può inviare una falsa risposta "NXDOMAIN" (dominio non esistente) a un resolver

Cosa DNSSEC non può fare

- DNSSEC non può proteggere contro:
  - Packet sniffing (del traffico DNS)
  - Attacchi di tipo DDoS
  - Alcune forme di phishing e pharming, ad esempio il typosquatting
- Inoltre non esegue controlli sui trasferimenti di zona dal nameserver master allo slave

DNSSEC e la riservatezza dei dati

- DNSSEC non garantisce la riservatezza dei dati
- La sua funzione principale è assicurare l'autenticità e l'integrità delle informazioni DNS, non di nasconderle
  - Il DNS rimane un database pubblico
  - DNSSEC non fa criptografia dei dati DNS
    - Il contenuto del pacchetto DNS resta integro. I dati vengono firmati digitalmente su ogni livello gerarchico dello spazio dei nomi

Utilizzo delle firme digitali

- Per garantire l'autenticità ed integrità dei dati, DNSSEC utilizza la criptografia asimmetrica: uso di chiavi pubbliche e private

- **Zone Signing Key (ZSK):** la ZSK privata è usata per generare firme digitali (RRSIG) per ogni Resource Record set di una zona. La ZSK pubblica è conservata nel file di zona per autenticare gli RRSIG

- **Key Signing Key(KSK):** la chiave KSK privata è usata per generare la firma digitale da associare sia alla ZSK pubblica sia alla KSK pubblica (Firma le DNSKEYs). La KSK pubblica viene anche utilizzata per la generazione del record DS che verrà depositato nella zona padre e che servirà ad autenticare la KSK pubblica indicata nella zona figlio

Nuovi Resource Records in DNSSEC

RRSIG (Firma digitale)

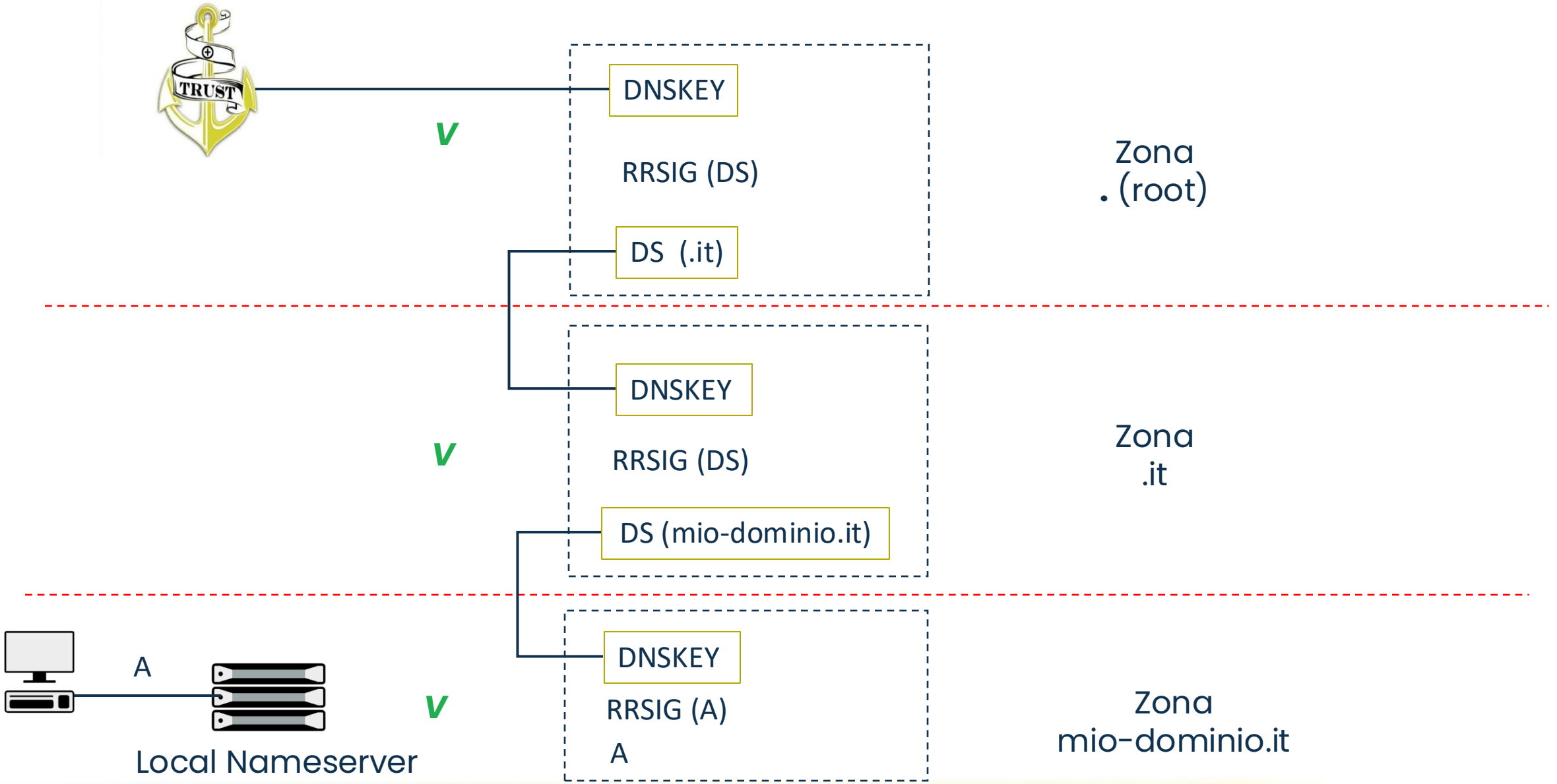
DNSKEY (Chiave pubblica)

DS (Delegations Signer, parent-child)

NSEC (prova di non esistenza)

NSEC3 (prova di non esistenza)

Processo di validazione di un Resource Record



Richiesta di attivazione di DNSSEC (1)

- Per abilitare DNSSEC su nomi a dominio .it e .eu già registrati con GARR, occorre farne richiesta scrivendo a nic@garr.it

- Per creare la “chain-of-trust” lungo la struttura gerarchica del DNS GARR dovrà aggiornare la registrazione del nome a dominio presso il database delle Authority dei TLD. A seconda che si tratti di un dominio .it o .eu sono disponibili due differenti procedure

Richiesta di attivazione di DNSSEC (2)

- **Per i domini .it**: chi gestisce il nameserver master della zona che si intende firmare, dovrà generare il record DS e trasmetterlo via email (nic@garr.it). GARR si occuperà di aggiornare la registrazione del dominio fornendo il record DS al Registro del ccTLD .it

- **Per i domini .eu**: chi gestisce il nameserver master della zona che si intende firmare, dovrà trasmettere via email a GARR la chiave pubblica associata alla zona firmata. GARR si occuperà di aggiornare la registrazione del dominio fornendo la chiave pubblica ad EURid che si occuperà a sua volta di generare il record DS

    - Anche nel caso in cui il servizio DNS sia gestito da terze parti, l'Utente che vuole abilitare DNSSEC sui propri domini dovrà comunicare record DS (.it) o chiave pubblica (.eu) a GARR

Gli Algoritmi supportati dalle Authority

Gli algoritmi supportati da EURid:

3 DSA/SHA-1
5 RSA/SHA-1
6 DSA-NSEC3-SHA1
7 RSASHA1-NSEC3-SHA1
8 RSA/SHA-256
10 RSA/SHA-512
13 ECDSAP256SHA256
14 ECDSAP384SHA384
15 ED25519
16 ED448

Gli algoritmi supportati dal Registro .it:

3 DSA/SHA-1
5 RSA/SHA-1
6 DSA-NSEC3-SHA1
7 RSASHA1-NSEC3-SHA1
8 RSA/SHA-256
10 RSA/SHA-512
12 ECC-GOST
13 ECDSAP256SHA256
14 ECDSAP384SHA384

Differenze nelle scelte algoritmiche

- Presenza degli algoritmi EdDSA (ED25519 e ED448) per .eu e l'algoritmo ECC-GOST per .it
  - Algoritmi EdDSA (supportati da .eu) questi sono algoritmi più moderni basati su curve ellittiche (https://www.youtube.com/watch?v=rzSU2m8oN48)
    - Offrono un eccellente rapporto tra sicurezza e prestazioni.
    - Hanno chiavi più piccole e sono molto efficienti dal punto di vista computazionale.
  - Algoritmo ECC-GOST (supportato da .it): questo algoritmo sebbene sia crittograficamente robusto, il suo uso è limitato e non è supportato su larga scala come altri algoritmi basati sulle curve ellittiche.

Strumenti online per il troubleshooting

- Verifica del corretto funzionamento/propagazione di DNSSEC:

http://dnsviz.net/

http://dnssec-debugger.verisignlabs.com/

http://dnscheck.iis.se/

https://stats.dnssec-tools.org/explore/

https://www.nic.it/it/gestisci-il-tuo-it/dns-check (solo per domini .it)

Conclusioni

- Per essere immuni da specifici attacchi su DNS è buona cosa attivare DNSSEC
  - Complessità di implementazione e gestione
  - Grandezza dei pacchetti DNS
  - Grandezza dei file di zona - Generazione e caricamento
  - Impatto delle query sulle performance di BIND
  - Attenzione al furto/smarrimento delle chiavi private

Informazioni online

- Tutte le informazioni per l'attivazione di DNSSEC per i domini .it e .eu registrati con GARR sono disponibili sul portale del GARR-NIC:
  - https://www.garr.it/it/servizi-garr/nomi-a-dominio#dnssec
- Per ulteriori informazioni scrivere a nic@garr.it

Grazie… Domande?

wooclap.com e codice WSGARR25