DNSSEC

The question

DNSSEC needs a maintained chain

Signed DNS data helps validating resolvers authenticate answers. Signing and parent delegation must stay coordinated.

01 Understand

02 Observe

03 Verify

A practical briefing for the people who own your domain.

DNSSEC

The mechanism

The resolver verifies signatures

It follows the chain of trust to check DNS data. DNSSEC authenticates data; it does not encrypt the query.

01 Signed authoritative DNS data

↓

02 Resolver checks chain of trust

↓

03 AD result reaches the scanner

The scanner observes Google Public DNS validation over HTTPS. It does not perform local DNSSEC cryptographic validation.

DNSSEC

The evidence

We report a resolver observation

> Our check reads Google Public DNS's authenticated-data result over HTTPS. Local cryptographic validation and other resolvers are outside this check.

PUT THE OBSERVATION IN CONTEXT

- **Public signal**
- **Service context**
- **Operational validation**

Use the finding to start an owned review.

DNSSEC

The handoff

Bring both domain owners together

Have the DNS operator and registrar administrator review signing, DS records and provider procedures before making changes.

BRING THE RIGHT OWNERS TOGETHER

01 DNS operator and registrar administrator

02 Domain operations

DNSSEC

Your checklist

Keep the DNSSEC operations checklist

- ✓ Check the chain
- ✓ Document rollovers
- ✓ Plan migrations
- ✓ Monitor validation

> Read the DNSSEC explainer and assign recovery ownership.
>
> **/learn/dnssec**