Panduan Aktivasi DNSSEC
Registrar Nama Domain Instansi Pemerintah
Versi 1.0 – 21 Januari 2026

DAFTAR ISI

Bab 1. Konsep Dasar DNSSEC

1.1 Pengertian DNSSEC

DNSSEC (*Domain Name System Security Extensions*) adalah fitur keamanan tambahan untuk memverifikasi keaslian data DNS. DNSSEC bekerja dengan cara menambahkan tanda tangan digital pada setiap data DNS untuk memastikan bahwa informasi yang diterima pengguna adalah benar dan belum diubah oleh pihak lain.

1.2 Fungsi Utama DNSSEC

Tujuan utama pengaktifan DNSSEC pada domain .go.id adalah:

- Autentikasi Data: Memastikan jawaban dari DNS Server berasal dari sumber yang sah.
- Integritas Data: Menjamin bahwa data DNS (seperti alamat IP server) tidak dimanipulasi saat proses pengiriman informasi.
- Perlindungan Trafik: Mencegah pengalihan trafik situs pemerintah ke alamat palsu yang berbahaya.

1.3 Komponen Data dalam DNSSEC

Untuk mengaktifkan DNSSEC di portal domain.go.id, Anda akan membutuhkan empat komponen data utama yang dihasilkan dari DNS Server Anda (cPanel/BIND9/PowerDNS):

1. Key Tag: Kode angka unik yang berfungsi sebagai identitas kunci DNSSEC.
2. Algorithm: Metode enkripsi yang digunakan untuk membuat tanda tangan digital (Contoh: RSA SHA256 atau ECDSA Curve P-256).
3. Digest Type: Jenis metode ringkasan (hashing) yang digunakan untuk data kunci (Contoh: SHA-256).
4. Digest: Deretan kode unik (fingerprint) hasil enkripsi dari kunci DNS Anda. Keempat data ini nantinya akan digabungkan menjadi sebuah DS Record.

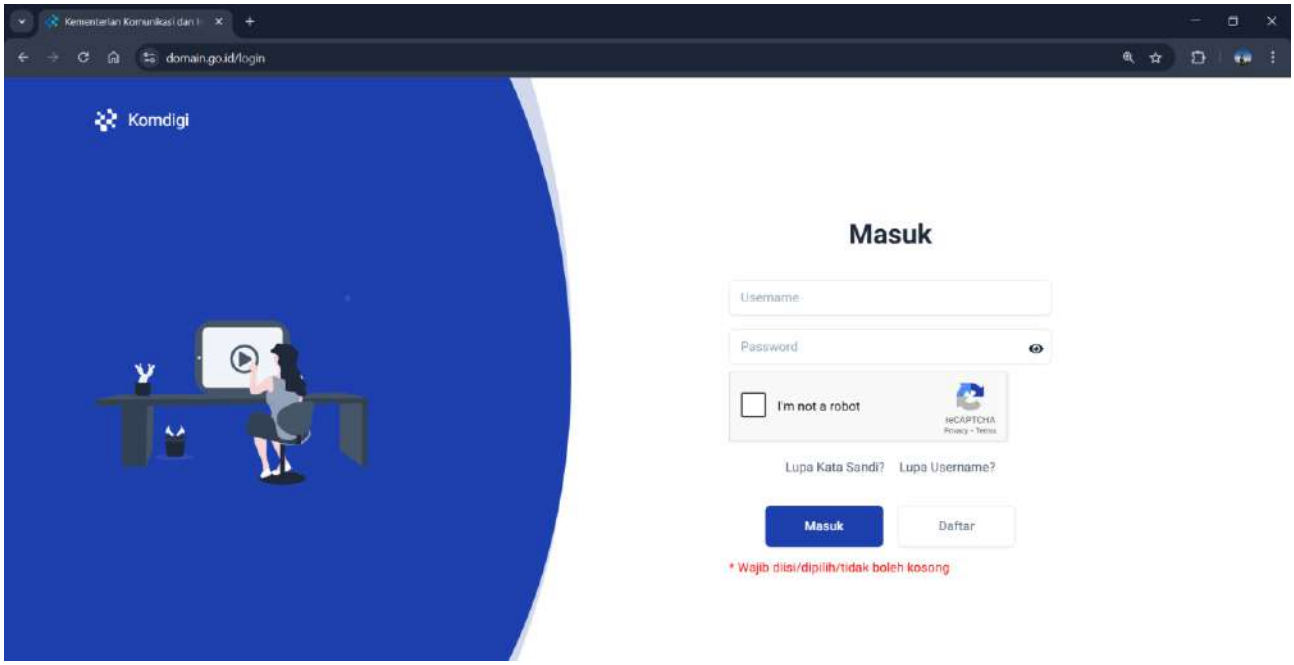
1.4 Cara Kerja DNSSEC dan Rantai Kepercayaan (Chain of Trust)

DNSSEC bekerja secara berantai. Agar DNSSEC Anda dianggap valid oleh dunia luar, data DS Record yang dihasilkan oleh DNS Server Anda harus didaftarkan ke pengelola domain (dalam hal ini melalui aplikasi portal domain.go.id). Jika data di server Anda cocok dengan data di portal domain.go.id, maka domain Anda resmi terproteksi.

Bab 2. Pengisian DNSSEC (DS Record) pada Aplikasi Domain.go.id

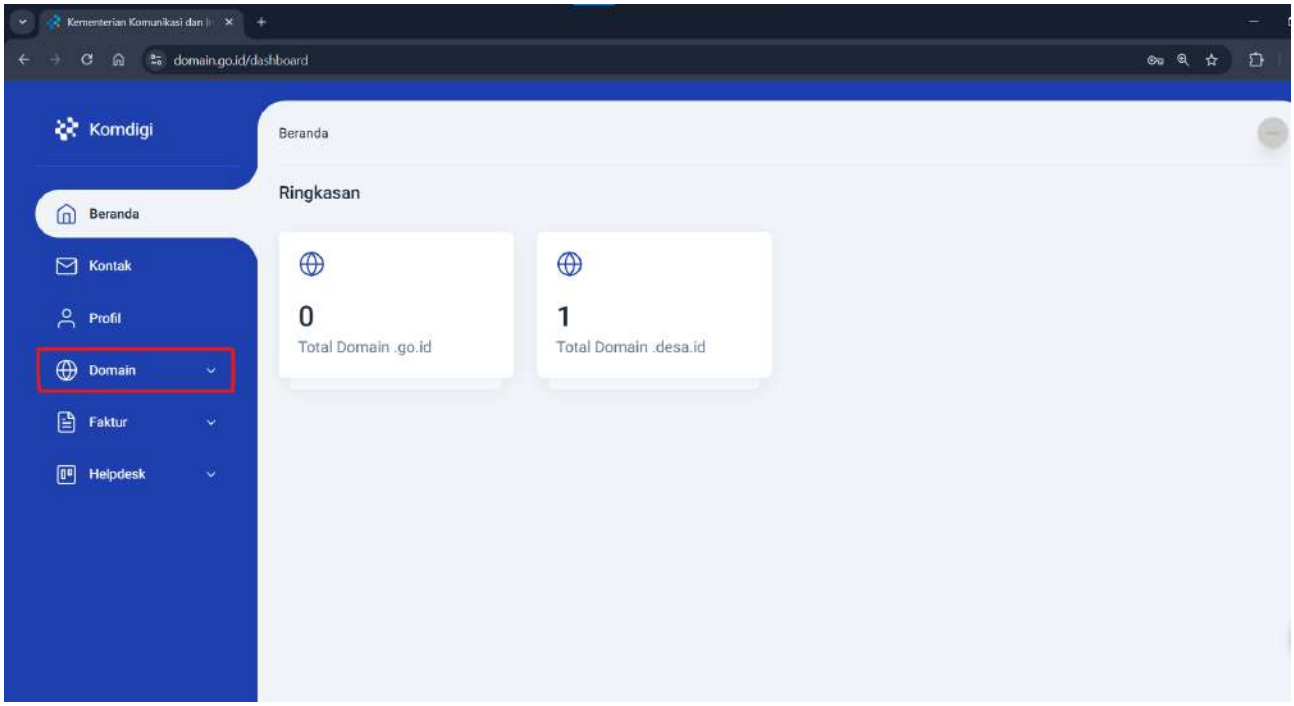
2.1 Login Akun Registrar

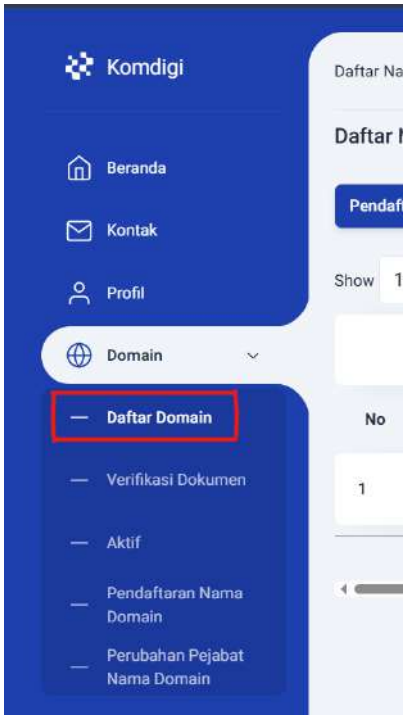
- Akses: https://domain.go.id/login
- Masuk ke akun registrar.



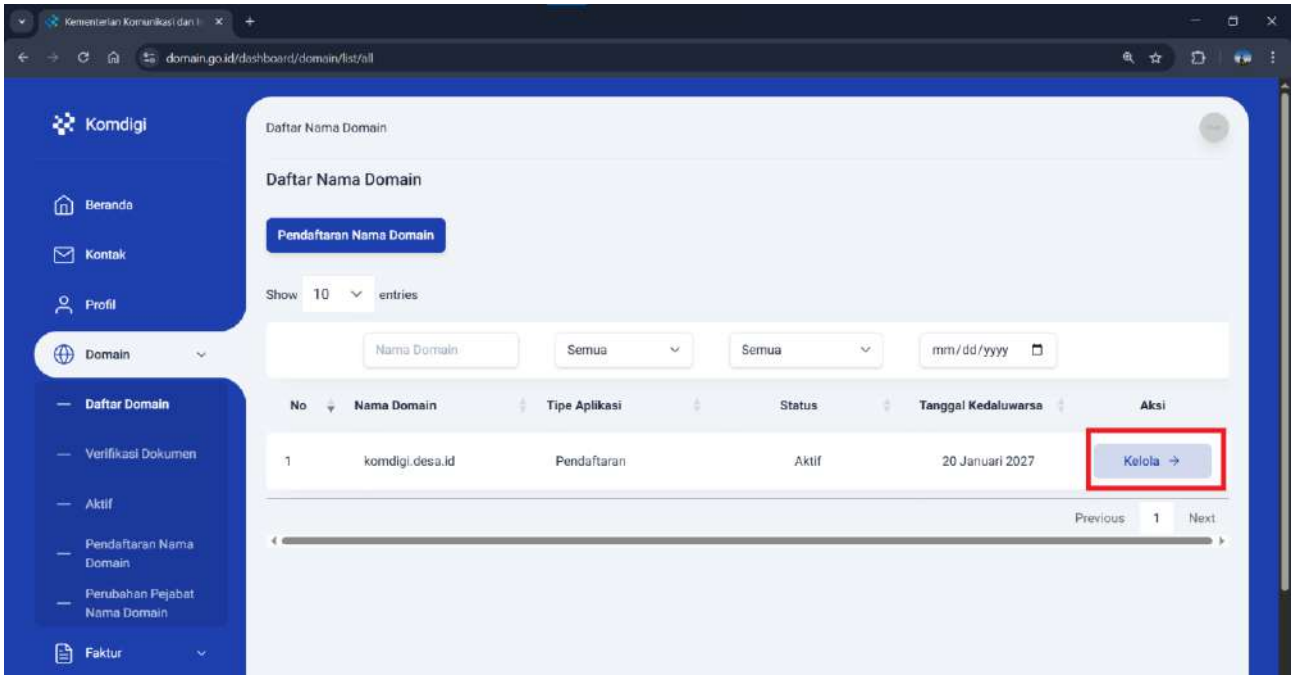
2.2 Masuk Menu “Domain”

- Pilih “Daftar Domain” di Menu “Domain”.



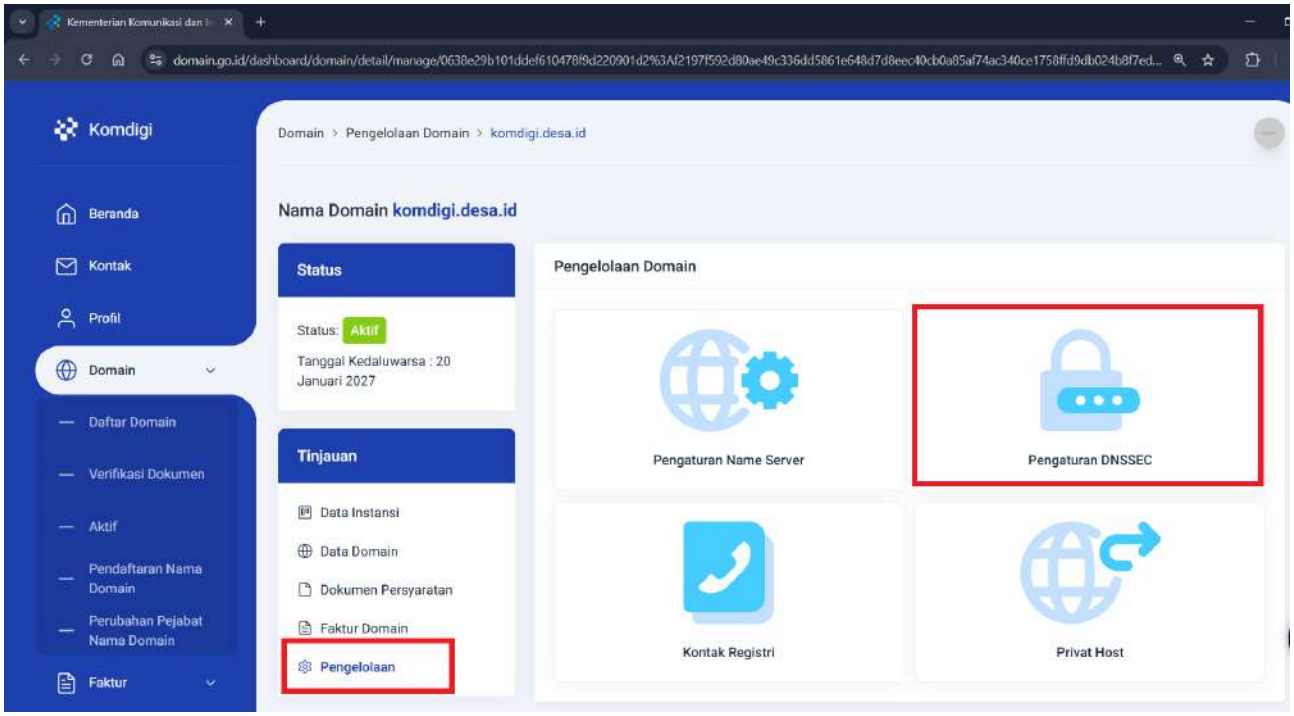


- Klik “Kelola” pada domain yang ingin diaktifkan fitur DNSSEC.



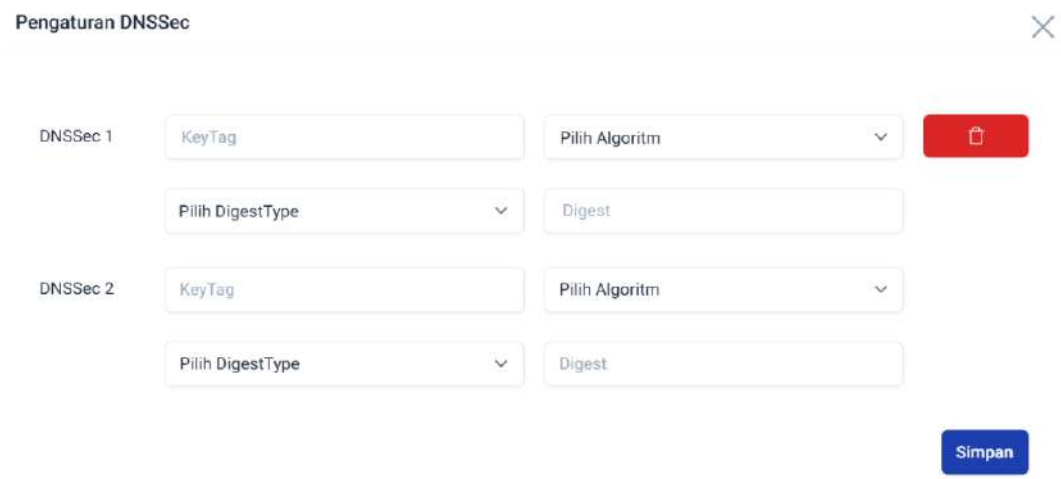
2.3 Pilih Menu “Pengaturan DNSSEC”

- Pilih “Pengelolaan” di menu “Tinjauan” dan klik “Pengaturan DNSSEC”



2.4 Masukkan DS Record

- Isi data yang sesuai dengan yang telah didapatkan
- Setelah diisi, klik Simpan.



2.5 Tunggu Propagasi

- Masa propagasi biasanya 10-30 menit untuk mulai aktif.

2.6 Verifikasi Status DNSSEC

Cek validasi melalui:

1. Verisign DNSSEC Analyzer → https://dnssec-debugger.verisignlabs.com/
2. DNSViz → DNSViz / https://dnsviz.net/

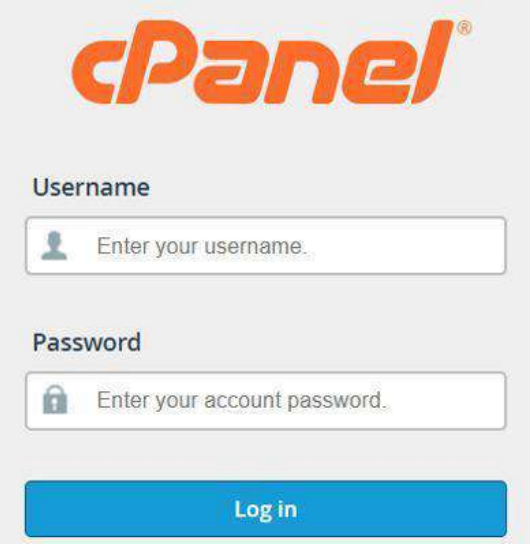
Jika status SECURE / VALID, DNSSEC berhasil diaktifkan.

Bab 3. Konfigurasi DNSSEC pada Server Hosting atau Provider DNS

Pada panduan ini, kami memberikan contoh generate key DNSSEC melalui cPanel yang disediakan oleh server hosting maupun penyedia server DNS.

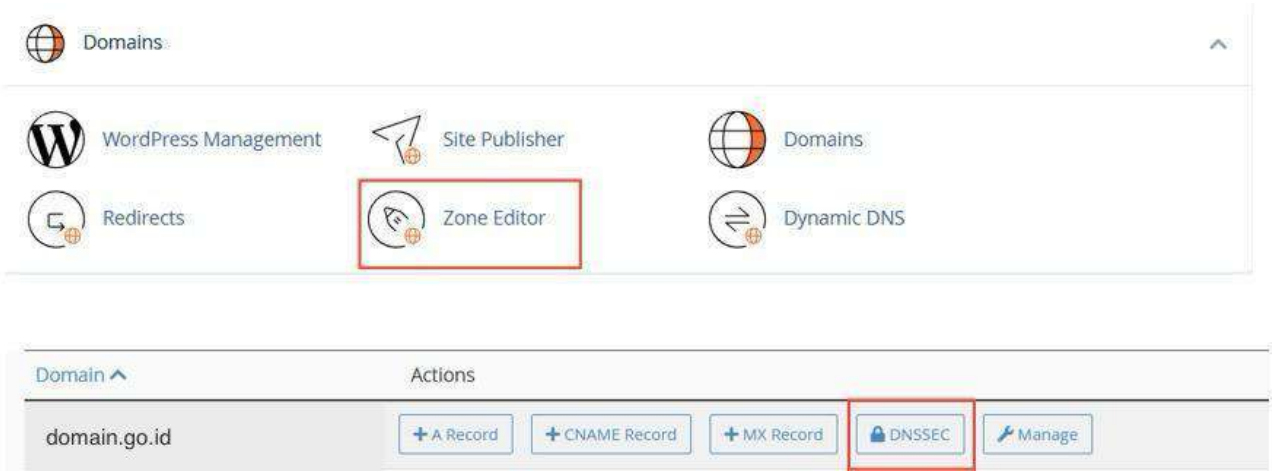
3.1 Login ke cPanel

- Masukkan username dan password, kemudian klik Log in



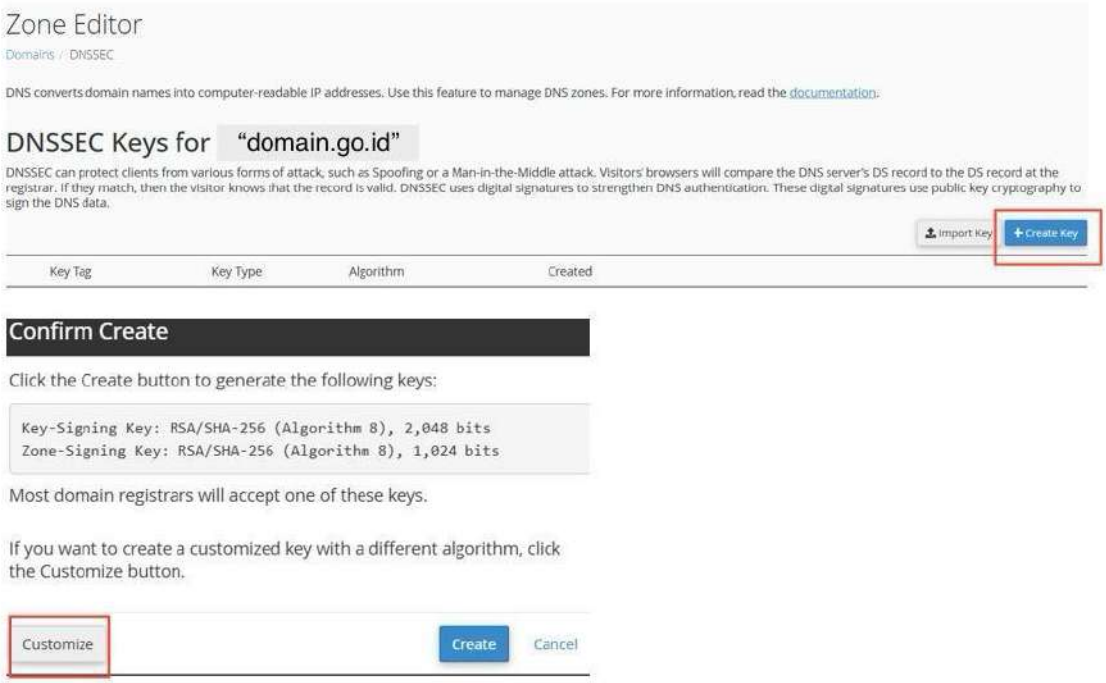
3.2 Buka Menu “Zone Editor”

- Pada dashboard → pilih Zone Editor
- Temukan domain Anda.
- Pada baris domain → klik tombol DNSSEC
- Jika opsi DNSSEC belum tersedia, hal ini menandakan bahwa fitur tersebut belum diaktifkan oleh penyedia hosting. Silakan mengajukan permintaan terlebih dahulu kepada pihak hosting agar DNSSEC dapat diaktifkan dan ditampilkan.

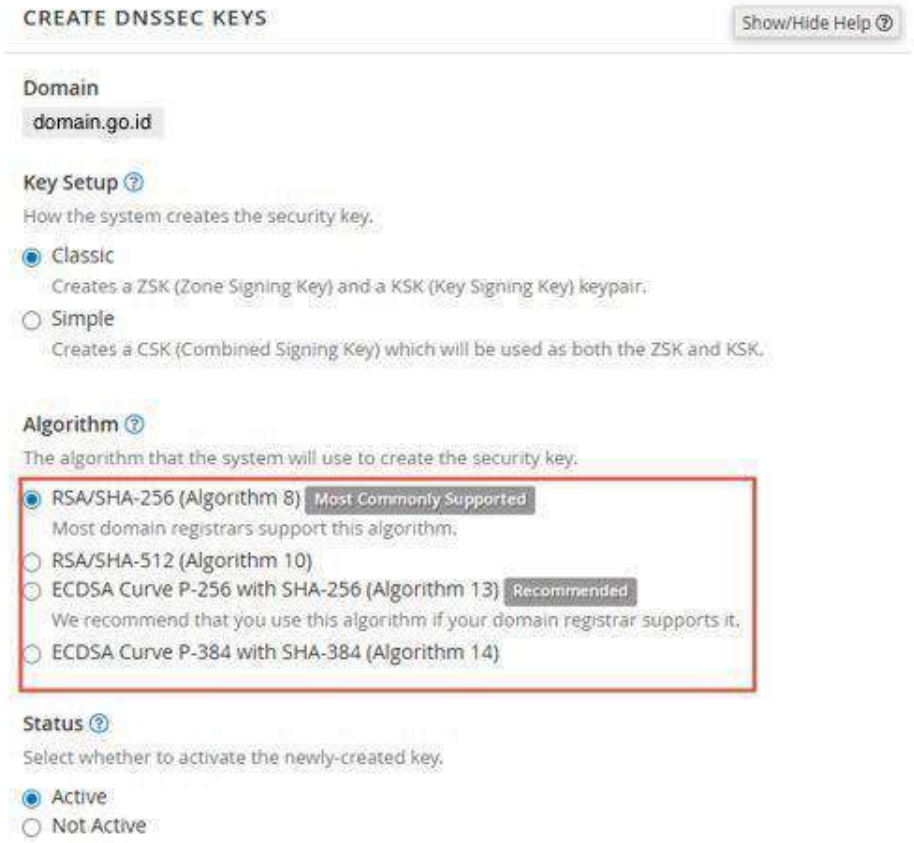


3.3 Generate DNSSEC Key

- Klik “Create Key”
- Kemudian Klik “Customize”



- Pilih Key Setup dan Algorithm



3.4 Salin DS Record

Setelah key dibuat, cPanel menampilkan data berikut:

- Key Tag, Algorithm, Digest Type, dan Digest
- Data ini akan digunakan pada domain.go.id.

Bab 4. Konfigurasi DNSSEC pada BIND9, PowerDNS, dan Unbound

Pada bab ini dicontohkan langkah-langkah pembuatan *key* DNSSEC pada DNS server yang banyak digunakan di internet, yaitu BIND9, Power DNS, dan Unbound.

4.1 Konfigurasi pada BIND9

4.1.1 Konfigurasi BIND9 agar berjalan sebagai Authoritative Server

- Edit file named.conf.options yang biasa terletak di /etc/bind dengan perintah sudo nano /etc/bind/named.conf.options
- Jika anda menggunakan distribusi Linux lain (seperti CentOS atau Fedora), lokasi file konfigurasi mungkin berbeda (biasanya berada di /etc/named.conf)

- Tambahkan script berikut ke dalam file named.conf.options anda.

```
forwarders {
        8.8.8.8;
        1.1.1.1;
 };
allow-query { any; };
dnssec-validation auto;
listen-on-v6 { none; };
```

- Pastikan jarak/indentation pada penulisan perintah tambahan pada file named.conf.options
- CTRL + O untuk save lalu CTRL + X untuk exit (lakukan save setiap kali melakukan perubahan)

4.1.2 Mengaktifkan DNSSEC secara otomatis

- Edit file named.conf.local dengan menjalankan perintah `sudo nano /etc/bind/named.conf.local`
- Tambahkan script berikut ke dalam file named.conf.local

```
zone "testing-server.my.id" {
        type master;
        file "/var/lib/bind/db.testing-server.my.id";
        dnssec-policy default;
        inline-signing yes;
};
```

- Catatan: Pastikan file `db.testing-server.my.id` berada di direktori `/var/lib/bind/` agar Bind9 memiliki izin tulis/write permission untuk membuat kunci

4.1.3 Pembuatan dan Pengecekan Zona

- Pastikan tidak ada typo atau salah ketik dengan menjalankan perintah `sudo named-checkconf`
  Jika tidak muncul pesan apa pun, berarti sudah benar
- Selanjutnya cek validitas file database zona domain Anda.
  jalankan perintah ini `sudo named-checkzone testing-server.my.id /var/lib/bind/db.testing-server.my.id`
  jika tidak ada masalah maka output yang dihasilkan adalah
  `zone testing-server.my.id/IN: loaded serial 2024011801`
  `OK`

- Restart BIND9 dengan perintah sudo systemctl restart named
  Jika tidak menghasilkan output, berarti sudah benar
- Cek apakah BIND9 sudah membuat kunci untuk DNSSEC,
  jalankan perintah dig @localhost DNSKEY testing-server.my.id +multiline
- pastikan status pada bagian HEADER menunjukkan NOERROR dan pada bagian ANSWER SECTION terlihat RRSIG, ini berarti konfigurasi dnssec-policy default telah bekerja sempurna.

4.1.4 Generate DS record

- Langkah terakhir adalah input DS Record ke panel domain
- Jalankan perintah dig @localhost DNSKEY testing-server.my.id | dnssec-dsfromkey -f - testing-server.my.id untuk melihat DS Record
- Seharusnya output yang dihasilkan adalah sebagai berikut
  namadomain.go.id IN DS 12345 13 2 abcdef1234567890…
- **Keterangan untuk Input ke Portal:**
  - **Key Tag:** 12345
  - **Algorithm:** 13 (biasanya defaultnya adalah ECDSA Curve P-256)
  - **Digest Type:** 2 (SHA-256)
  - **Digest:** abcdef1234567890... (salin seluruh kode panjang tersebut)

4.2 Konfigurasi pada PowerDNS

Bagian ini ditujukan bagi admin yang menggunakan PowerDNS sebagai *Authoritative DNS Server*. Pengaturan DNSSEC di PowerDNS dilakukan secara otomatis setelah perintah aktivasi dijalankan.

Berikut catatan penting sebelum melakukan aktivasi DNSSEC Power DNS pada panduan ini

- **Backend SQLite3:** Panduan ini mengasumsikan Anda menggunakan SQLite3 sebagai database PowerDNS karena pengelolaannya yang jauh lebih mudah dibandingkan MySQL/PostgreSQL.
- **Izin Akses (Permissions):** User sistem **pdns** harus memiliki hak akses penuh (read/write) pada folder tempat database disimpan (biasanya di **/var/lib/powerdns/**).
- **Versi Software:** Pastikan Anda menggunakan PowerDNS versi terbaru (Authoritative Server) untuk memastikan fitur **pdnsutil** sudah mendukung perintah otomatis.

Sebelum memulai, pastikan anda sudah masuk ke admin/root server di CLI.

4.2.1 Penyesuaian Konfigurasi Utama

Sebelum menjalankan perintah DNSSEC, Anda harus memberikan izin pada PowerDNS agar fitur keamanan ini diaktifkan di tingkat sistem.

- buka file konfigurasi PowerDNS biasanya terletak di /etc/powerdns/pdns.conf

  menggunakan command:

```
nano /etc/powerdns/pdns.conf
```

- Cari bagian konfigurasi backend dan pastikan baris **gsqlite3-dnssec=yes** sudah ditambahkan:

```
launch=gsqlite3
gsqlite3-database=/var/lib/powerdns/pdns.sqlite3
gsqlite3-dnssec=yes
```
→ Pastikan bagian ini sudah ditambahkan pada file konfigurasi

- Simpan (Ctrl+O, Enter) dan keluar (Ctrl+X).

- Restart layanan untuk menerapkan perubahan:

```
systemctl restart pdns
```

4.2.2 Membuat Zona Domain

- Jika Anda baru saja menginstal PowerDNS, buatlah zona domain Anda terlebih dahulu, gunakan perintah `pdnsutil secure-zone` diikuti dengan nama domain anda.

```
pdnsutil create-zone instansianda.go.id
```

- Ubah `instansianda` menjadi nama domain anda

4.2.3 Aktivasi DNSSEC (Secure Zone)

- Mengaktifkan tanda tangan digital pada domain Anda.

```
pdnsutil secure-zone instansianda.go.id
```

4.2.4 Sinkronisasi Data (Rectify Zone)

Langkah ini wajib dilakukan setiap kali ada perubahan pada zona atau setelah aktivasi DNSSEC agar seluruh data DNS Anda memiliki tanda tangan digital yang valid.

- Gunakan perintah:

```
pdnsutil rectify-zone instansianda.go.id
```

4.2.5 Mendapatkan DS Record untuk Portal domain.go.id

- Jalankan perintah di bawah untuk menampilkan informasi kunci yang harus dimasukkan ke portal pendaftaran domain

```
pdnsutil show-zone instansianda.go.id
```

- Setelah menjalankan perintah di atas cari bagian yang tertulis **DS Records**
- Anda akan melihat informasi seperti berikut:

  Contoh:

  ```
  instansianda.go.id. IN DS 56789 13 2 abcdef1234567890
  ```

- **Keterangan untuk Input ke Portal:**
  - **Key Tag:** 56789
  - **Algorithm:** 13 (biasanya defaultnya adalah ECDSA Curve P-256)
  - **Digest Type:** 2 (SHA-256)
  - **Digest:** abcdef1234567890... (salin seluruh kode panjang tersebut)

4.3 Konfigurasi pada Unbound

Bagian ini ditujukan bagi admin yang menggunakan Unbound sebagai *Validator DNS Server*. Pengaturan DNSSEC yang sudah dibuat menggunakan BIND9 atau PowerDNS divalidasi dengan Unbound.

4.3.1 Membuat file konfigurasi baru

- Jalankan perintah `sudo nano /etc/unbound/unbound.conf.d/dnssec.conf` untuk membuat dan edit file dnssec.conf
- Isi file konfigurasi dengan script berikut.

```
server:
        # --- 1. PENGATURAN JARINGAN ---
        # HANYA mendengarkan di Localhost (127.0.0.1)
        # Ini PENTING agar tidak bentrok dengan BIND9 di IP Publik
        interface: 127.0.0.1
        port: 53
        # Protokol yang diizinkan
        do-ip4: yes
        do-udp: yes
        do-tcp: yes

# --- 2. KEAMANAN & AKSES ---
        # Hanya izinkan localhost yang bertanya ke Unbound
        access-control: 127.0.0.0/8 allow
        access-control: 0.0.0.0/0 refuse
        # Mencegah Warning: Izinkan Unbound bertanya ke alamat lokal (BIND9)
        do-not-query-localhost: no
        # --- 3. MODUL VALIDASI DNSSEC ---
        # Mengaktifkan modul validator
        module-config: "validator iterator"
        auto-trust-anchor-file: "/var/lib/unbound/root.key"
```

```
        # --- 4. JEMBATAN KE BIND9 (STUB ZONE) ---
        # Jika ada yang tanya soal domain kita, lempar ke BIND9 di port 5353
stub-zone:
        name: "testing-server.my.id"
        stub-addr: 127.0.0.1@5353
```

- **interface: 127.0.0.1**: Mengunci Unbound agar hanya hidup di dalam server, tidak terekspos ke internet.
- **do-not-query-localhost: no**: Wajib diset no. Jika tidak, Unbound akan menolak meneruskan pertanyaan ke BIND9 yang berada di IP lokal yang sama.
- **stub-addr: 127.0.0.1@5353**: Ini adalah "pintu belakang". Unbound akan mengetuk BIND9 di port 5353 khusus untuk domain Anda.
- Jalankan perintah unbound-checkconf untuk melihat jika ada typo pada penulisan script file dnssec.conf. jika setelah perintah dijalankan tidak menghasilkan apapun berarti tidak ada salah ketik pada file dnssec.conf

4.3.2 Verifikasi Unbound sudah berjalan dengan benar

- Pastikan status Unbound aktif, jalankan perintah sudo systemctl status unbound
  jika semua berjalan benar, seharusnya tidak ada status error yang dilaporkan dan terlihat status Active berwarna hijau.
- Terakhir, jalankan perintah dig @127.0.0.1 testing-server.my.id +dnssec untuk melihat apakah DNSSEC yang sudah aktif sebelumnya sudah divalidasi oleh Unbound
- Pada bagian flags, jika terlihat ada “ad” berarti setup Unbound berhasil memvalidasi DNSSEC yang aktif

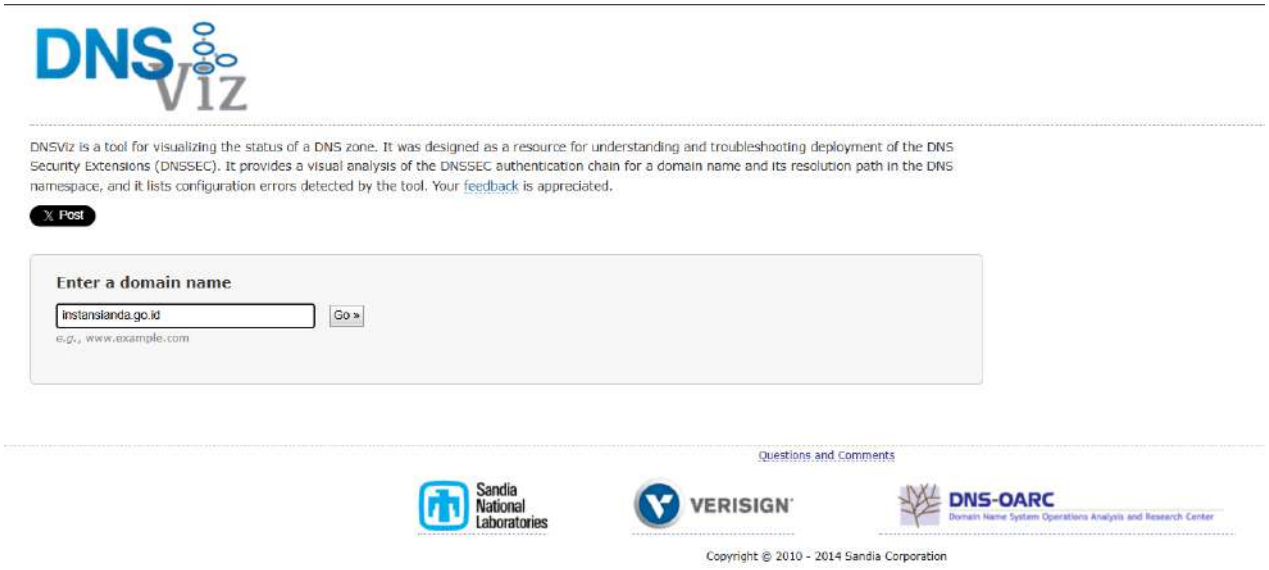
Bab 5. Pengujian, Perawatan, dan Pemecahan Masalah

5.1 Pengujian Menggunakan DNSSEC Analyzer

Cara termudah untuk melakukan validasi adalah menggunakan alat penguji daring (online). Alat ini akan memetakan koneksi keamanan dari *Root Server*, ke TLD (.id), ke SLD (.go.id), hingga ke nama domain Anda.

- Buka situs **DNSViz.net** atau **DNSSEC Analyzer (Verisign)**.

- Masukkan nama domain Anda (contoh: instansianda.go.id) pada kolom pencarian.



- Klik tombol **Analyze** atau **Go**.

- Cara Membaca Hasil:
    - **Warna Hijau/Centang Biru:** Berarti DNSSEC valid dan rantai kepercayaan tersambung dengan benar.
    - **Warna Merah/Tanda Silang:** Berarti ada kegagalan verifikasi. Biasanya terjadi karena data di portal domain.go.id tidak cocok dengan data di server DNS Anda.

5.2 Pengecekan Mandiri via Terminal (dig)

Anda bisa memastikan server DNS sudah mengeluarkan tanda tangan digital secara langsung melalui perintah terminal:

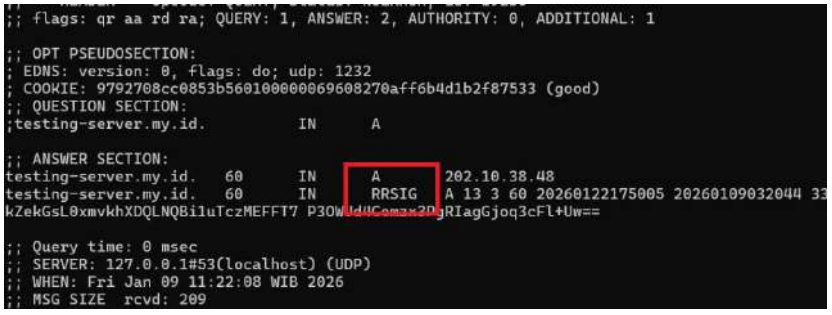
- **Cek Tanda Tangan Digital**

  gunakan perintah:

  `dig +dnssec nama-instansi.go.id`

- Pastikan anda sudah masuk sebagai admin/root sebelum menjalankan perintah

Contoh:

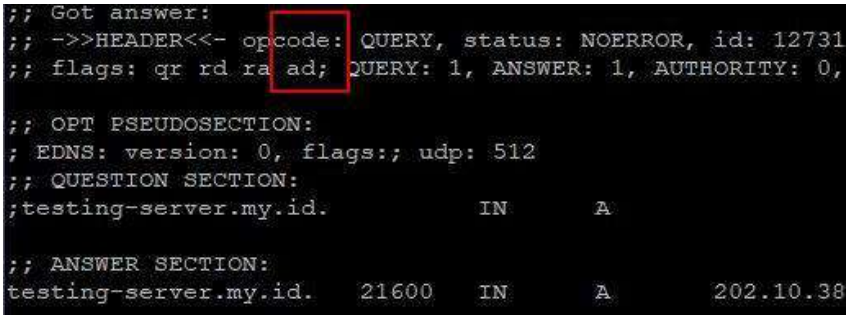


- (Cek pada kolom **ANSWER SECTION**, harus muncul baris **RRSIG**).
- **Cek Validitas Global**

  gunakan perintah:

  dig domainanda.go.id

Contoh:



- (Cek pada kolom **flags**, pastikan muncul kode **ad** yang berarti Authenticated Data).

5.3 Pemeliharaan Rutin (*Maintenance*)

DNSSEC memerlukan pemeliharaan agar tidak terjadi kegagalan akses domain secara tiba-tiba.

1. **Otomatisasi Tanda Tangan (Re-signing):** Pastikan layanan DNS (BIND9/PowerDNS/Unbound) tetap aktif. Sistem secara otomatis akan memperbarui tanda tangan digital sebelum masa berlakunya habis.
2. **Pembaruan Kunci (Key Rollover):** Disarankan untuk memperbarui kunci DNSSEC (KSK/ZSK) secara berkala (misalnya 1 tahun sekali). Jika kunci diperbarui di server, Anda **wajib** memperbarui data DS Record di portal domain.go.id agar domain tidak mati.
3. **Backup Data Kunci:** Selalu simpan salinan cadangan (*backup*) file kunci DNSSEC Anda. Kehilangan kunci privat akan menyebabkan domain Anda gagal divalidasi oleh internet.
4. **Prosedur Migrasi:** Jika ingin pindah server, nonaktifkan (hapus) dulu DS Record di portal domain.go.id, pindahkan server, baru aktifkan kembali DNSSEC di server yang baru.

5.4 Penanganan Masalah (*Troubleshooting*)

Gejala Masalah	Kemungkinan Penyebab	Solusi
Domain tidak bisa diakses sama sekali.	Data DS Record di portal tidak cocok dengan kunci di server.	Hapus DS Record di portal domain.go.id sementara agar domain hidup kembali, lalu cek ulang kunci

		server.
Status "Bogus" pada pengujian online.	Masa berlaku tanda tangan digital (*RRSIG*) sudah kadaluarsa.	Jalankan perintah *rectify* atau restart layanan DNS agar server melakukan *signing* ulang.
Perubahan data DNS tidak terbaca.	Cache DNS masih menyimpan data lama.	Tunggu masa propagasi (1-2 jam) atau lakukan pembersihan cache pada resolver.

Tindakan Darurat: Jika terjadi gangguan akses yang luas setelah aktivasi, segera hapus data DS Record di portal domain.go.id. Ini akan mengembalikan domain ke status normal (non-DNSSEC) dalam waktu singkat.