

Panduan Aktivasi DNSSEC

Registrar Nama Domain Instansi Pemerintah

Versi 1.0 – 21 Januari 2026

DAFTAR ISI

Bab 1. Konsep Dasar DNSSEC	2
1.1 Pengertian DNSSEC	2
1.2 Fungsi Utama DNSSEC.....	2
1.3 Komponen Data dalam DNSSEC	2
1.4 Cara Kerja DNSSEC dan Rantai Kepercayaan (Chain of Trust).....	2
Bab 2. Pengisian DNSSEC (DS Record) pada Aplikasi Domain.go.id.....	2
2.1 Login Akun Registrar.....	2
2.2 Masuk Menu “Domain”	3
2.3 Pilih Menu “Pengaturan DNSSEC”	4
2.4 Masukkan DS Record	5
2.5 Tunggu Propagasi	5
2.6 Verifikasi Status DNSSEC.....	5
Bab 3. Konfigurasi DNSSEC pada Server Hosting atau Provider DNS.....	6
3.1 Login ke cPanel.....	6
3.2 Buka Menu “Zone Editor”	6
3.3 Generate DNSSEC Key	7
3.4 Salin DS Record.....	8
Bab 4. Konfigurasi DNSSEC pada BIND9, PowerDNS, dan Unbound.....	9
4.1 Konfigurasi pada BIND9	9
4.2 Konfigurasi pada PowerDNS.....	11
4.3 Konfigurasi pada Unbound	13
Bab 5. Pengujian, Perawatan, dan Pemecahan Masalah	14
5.1 Pengujian Menggunakan DNSSEC Analyzer.....	14
5.2 Pengecekan Mandiri via Terminal (dig)	15
5.3 Pemeliharaan Rutin (<i>Maintenance</i>)	16
5.4 Penanganan Masalah (<i>Troubleshooting</i>).....	16

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.

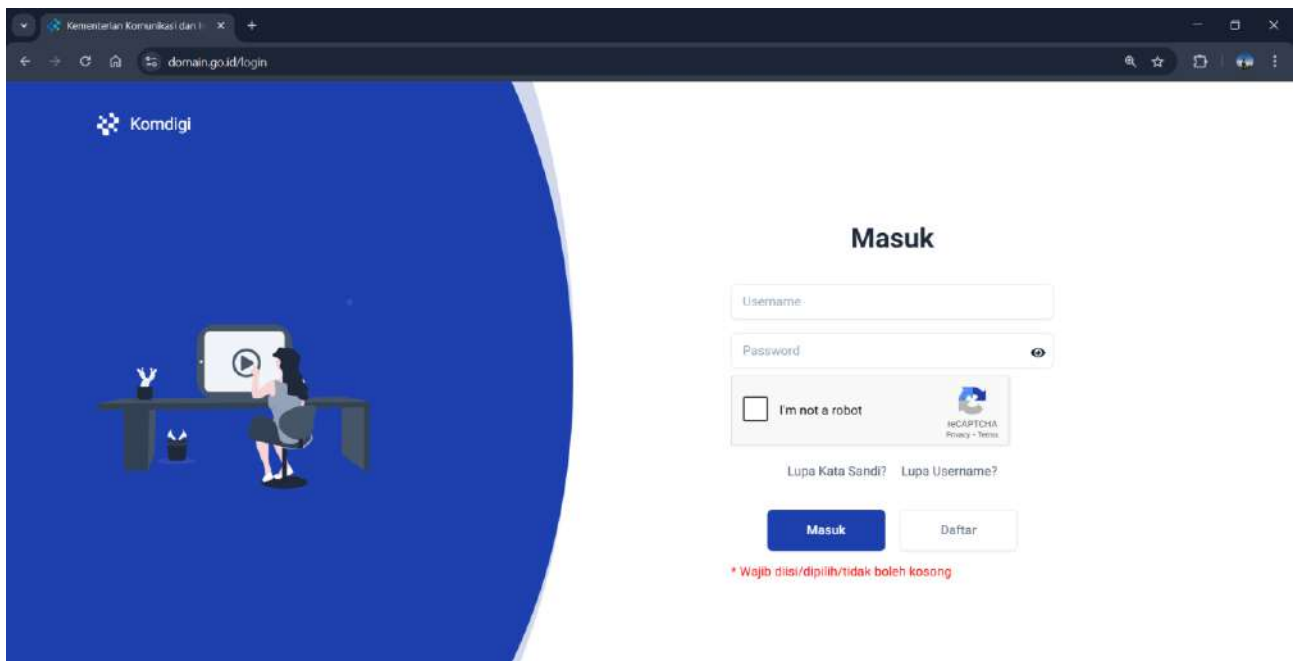
1.4 Cara Kerja DNSSEC dan Rantai Kepercayaan (Chain of Trust)

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

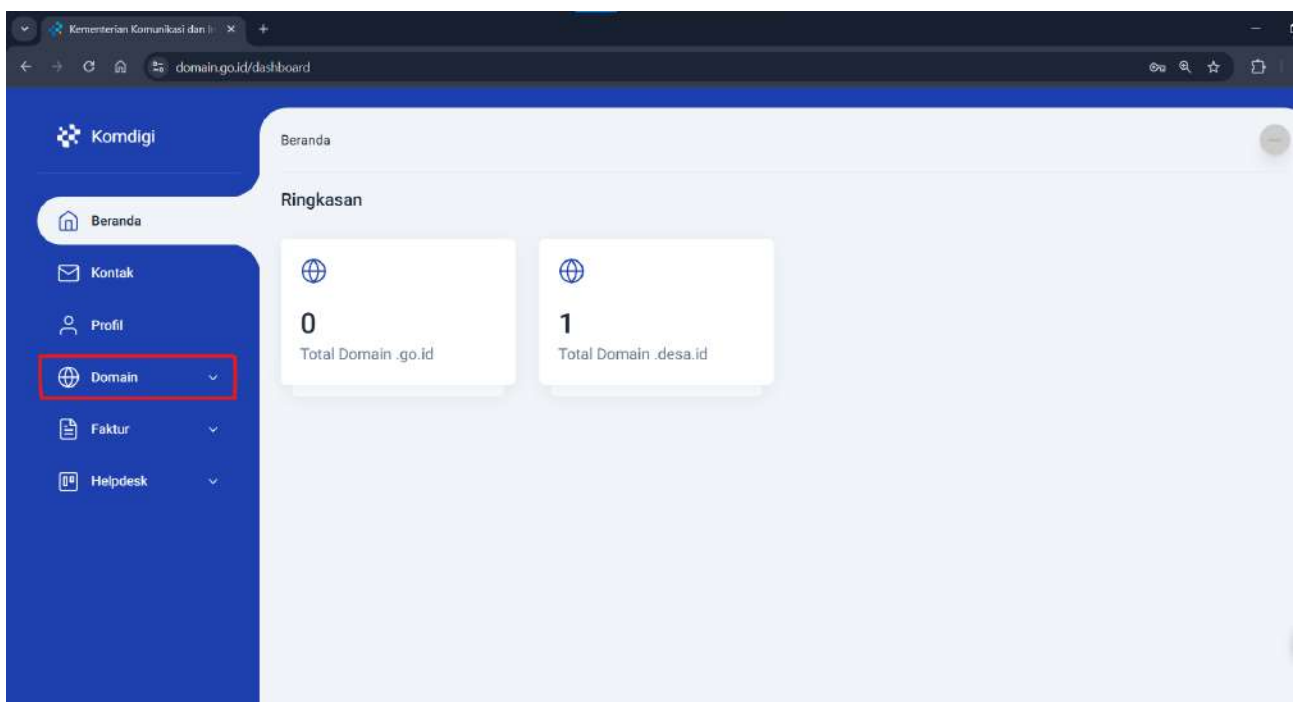
2.1 Login Akun Registrar

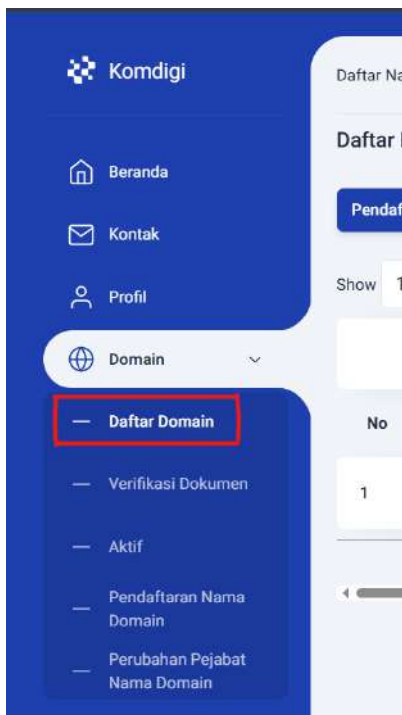
- **Akses:** <https://domain.go.id/login>
- Masuk ke akun registrar.



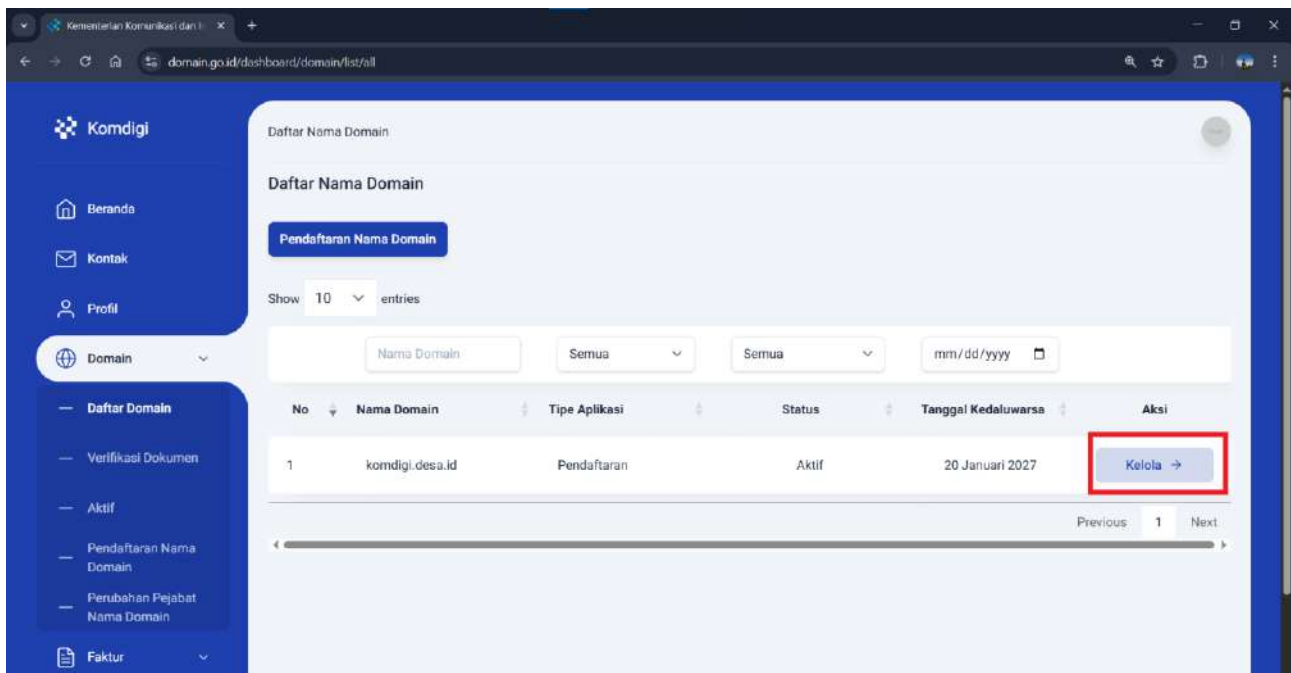
2.2 Masuk Menu “Domain”

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



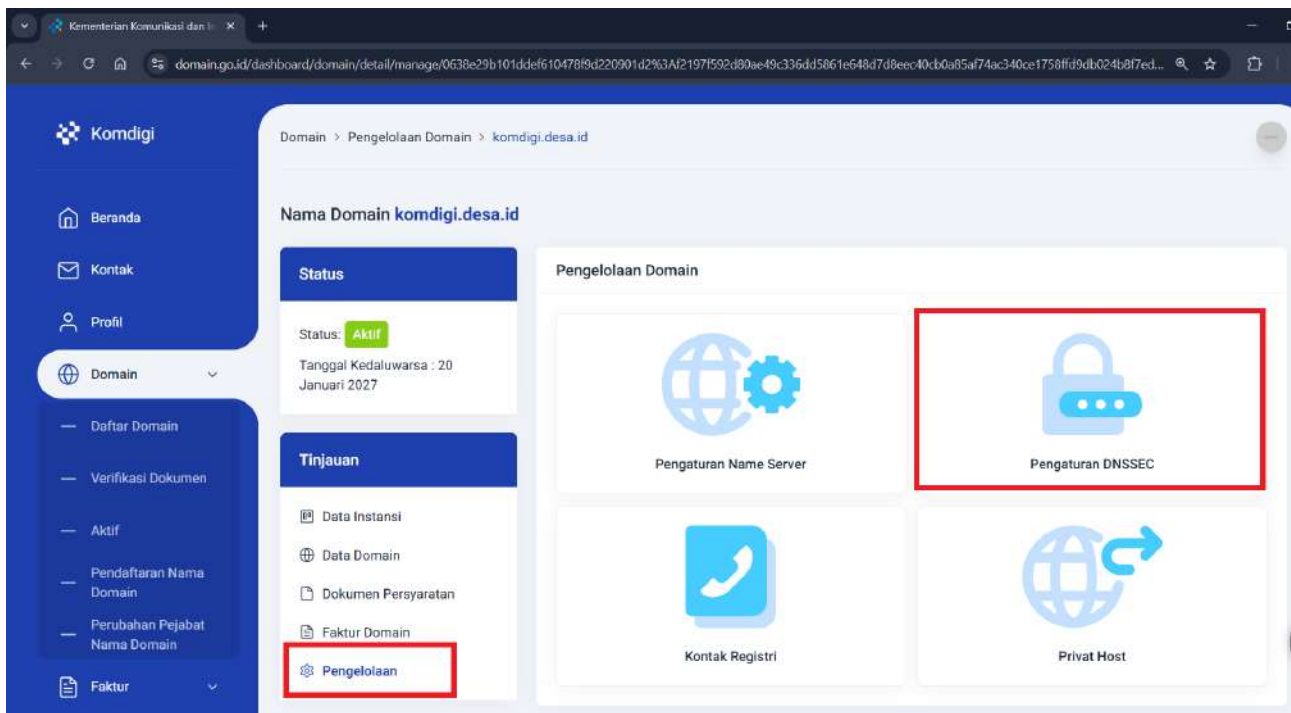


- Klik “Kelola” pada domain yang ingin diaktifkan fitur DNSSEC.



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.

Pengaturan DNSSEC

DNSSec 1	KeyTag	Pilih Algoritma	
	Pilih DigestType	Digest	
DNSSec 2	KeyTag	Pilih Algoritma	
	Pilih DigestType	Digest	



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 → [DNSTViz](https://dnsviz.net/) / <https://dnsviz.net/>

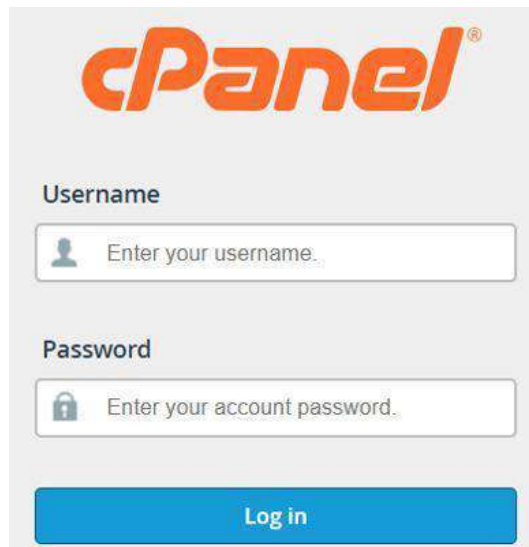
Jika status SECURE / VALID, DNSSEC berhasil diaktifkan.

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.

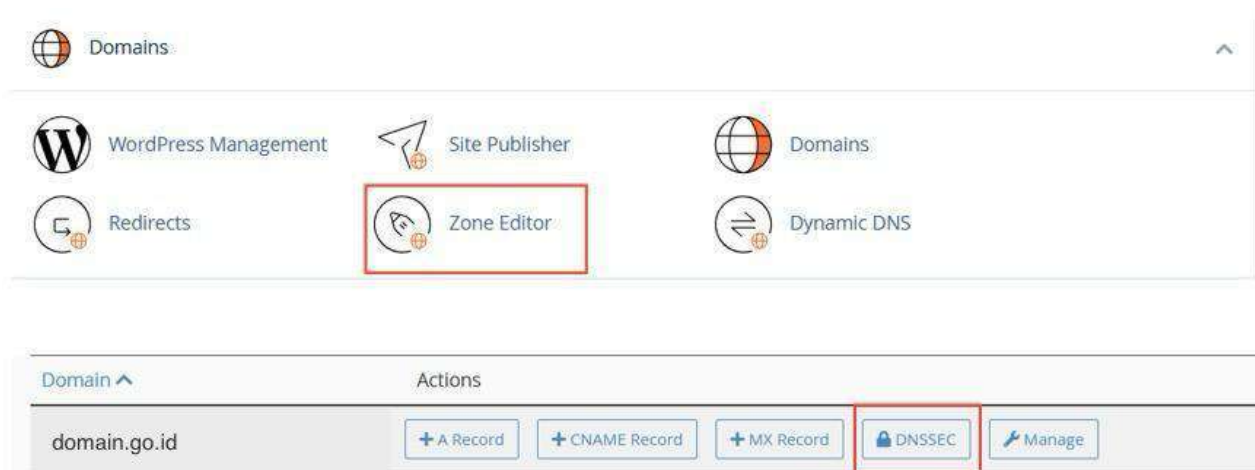
3.1 Login ke cPanel

- Masukkan username dan password, kemudian klik Log in

The image shows the cPanel login interface. At the top is the orange cPanel logo. Below it, there are two input fields: one for 'Username' with a user icon and placeholder text 'Enter your username.', and one for 'Password' with a lock icon and placeholder text 'Enter your account password.'. At the bottom of the form is a blue button labeled 'Log in'.

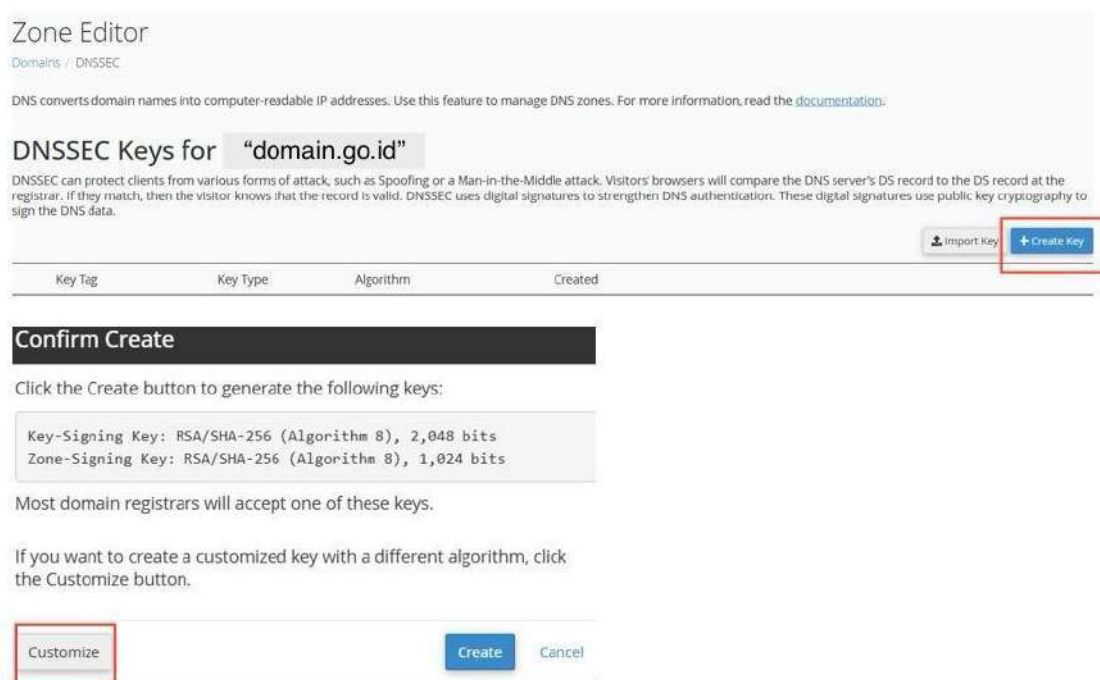
3.2 Buka Menu “Zone Editor”

- 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

CREATE DNSSEC KEYS

Show/Hide Help ?

Domain

domain.go.id

Key Setup ?

How the system creates the security key.

☒ Classic

Creates a ZSK (Zone Signing Key) and a KSK (Key Signing Key) keypair.

☐ Simple

Creates a CSK (Combined Signing Key) which will be used as both the ZSK and KSK.

Algorithm ?

The algorithm that the system will use to create the security key.

☒ RSA/SHA-256 (Algorithm 8) **Most Commonly Supported**

Most domain registrars support this algorithm.

☐ RSA/SHA-512 (Algorithm 10)

☐ ECDSA Curve P-256 with SHA-256 (Algorithm 13) **Recommended**

We recommend that you use this algorithm if your domain registrar supports it.

☐ ECDSA Curve P-384 with SHA-384 (Algorithm 14)

Status ?

Select whether to activate the newly-created key.

☒ Active

☐ Not Active

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.

DNSSEC KEY DETAILS



Information: To enable DNSSEC for your domain, you must go to your domain registrar website and use the information below to fill out their DNSSEC forms.

Domain

domain.go.id

Key Tag

64141

Algorithm

RSA/SHA-256 2,048 bits (Algorithm 8)

Created

Nov 25, 6:05:25 AM

The following digests are available:

Digest Type

SHA-1 (Algorithm 1)

Digest

65e35e561b4c01cc

[Copy](#)

Digest Type

SHA-256 (Algorithm 2)

Digest

aec2b2c1e9efee3b1a03597eb0ea8ee255b9fb0a1

[Copy](#)

Digest Type

SHA-384 (Algorithm 4)

Digest

977de0559e4fd27cb46f290abad5ec464481a1d3b37595d527c9025

2c86f1d32ec3f8f134

[Copy](#)

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 **sqlite3-dnssec=yes** sudah ditambahkan:

```
launch=sqlite3
```

```
sqlite3-database=/var/lib/powerdns/pdns.sqlite3
```

```
sqlite3-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 [DNSTViz.net](https://dnsviz.net) atau [DNSSEC Analyzer \(Verisign\)](https://dnssec-analyzer.verisign.com).
- Masukkan nama domain Anda (contoh: **instansianda**.go.id) pada kolom pencarian.



DNSviz is a tool for visualizing the status of a DNS zone. It was designed as a resource for understanding and troubleshooting deployment of the DNS Security Extensions (DNSSEC). It provides a visual analysis of the DNSSEC authentication chain for a domain name and its resolution path in the DNS namespace, and it lists configuration errors detected by the tool. Your [feedback](#) is appreciated.

Post

Enter a domain name

instansianda.go.id

Go »

e.g., www.example.com

[Questions and Comments](#)



Copyright © 2010 - 2014 Sandia Corporation

- 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:

```
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: do; udp: 1232
;; COOKIE: 9792708cc0853b560100000069608270aff6b4d1b2f87533 (good)
;; QUESTION SECTION:
testing-server.my.id.      IN      A
;; ANSWER SECTION:
testing-server.my.id.     60      IN      A      202.10.38.48
testing-server.my.id.     60      IN      RRSIG   A 13 3 60 20260122175005 20260109032044 33
kZekGsl0xmvkhXQQLNQBiluTczMEFFT7 P30WldwCmaw2DgRIagGjoq3cFl+Uw==
;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(localhost) (UDP)
;; WHEN: Fri Jan 09 11:22:08 WIB 2026
;; MSG SIZE rcvd: 209
```

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

gunakan perintah:

dig domainanda.go.id

Contoh:

```
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12731
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0,
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;testing-server.my.id.      IN      A
;; ANSWER SECTION:
testing-server.my.id.      21600   IN      A      202.10.38
```

- (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 (<i>RRSIG</i>) sudah kadaluarsa.	Jalankan perintah <i>rectify</i> atau restart layanan DNS agar server melakukan <i>signing</i> 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.