BigLinux og Secure Boot - Komplet guide

BigLinux understøtter officielt ikke kørsel med Secure Boot aktiveret, uanset det grafiske miljø (KDE, GNOME, Cinnamon eller Xfce).

For at installere eller køre BigLinux skal du deaktivere Secure Boot i din computers BIOS/UEFI. Valget af grænseflade påvirker ikke dette krav, da begrænsningen ligger i systeminitialiseringen (bootloader) og ikke i skrivebordsmiljøet.

Hvad er Secure Boot?

Det er en UEFI-sikkerhedsfunktion, der verificerer, at operativsystemet har en gyldig digital signatur (normalt fra Microsoft), før det tillader opstart. Dette hjælper med at forhindre malware i at indlæses før systemet.

Hvordan fungerer andre distributioner?

Linux-distributioner som Ubuntu, Fedora og Linux Mint bruger et program kaldet SHIM, som er signeret af Microsoft og fungerer som en "autorisator" for resten af systemet med Secure Boot aktiveret.

Og BigLinux?

Da BigLinux er afledt af Manjaro/Arch Linux, bruger det ikke den Microsoft-signerede SHIM. I praktiske tests med Secure Boot aktiveret starter BigLinux ikke, fordi bundkortets firmware ikke genkender dens bootloader som troværdig.

✅ Officiel løsning: Deaktiver sikker opstart

Trin-for-trin vejledning

Trin 1: Få adgang til BIOS/UEFI

Genstart din computer

Når skærmen bliver mørk, skal du gentagne gange trykke på den specifikke tast for din producent:

Dell, Acer, ASUS: F2 eller Del
HP: F10 eller Esc
Lenovo: F1 eller F2 (eller Novo-tasten)
Samsung: F2

Toshiba: F2 eller Esc
Samlede computere: Del (mest almindelige)

Trin 2: Find funktionen Sikker opstart

Den nøjagtige placering varierer afhængigt af producenten, men den er normalt i en af disse faner:

Opstart
Sikkerhed
Godkendelse
UEFI-indstillinger

Se efter termer som:

Sikker opstart
Kontrol af sikker opstart

Trin 3: Deaktiver

Skift status til Deaktiveret

Hvis der er muligheder som Standard og Brugerdefineret, skal du vælge Deaktiveret

Trin 4: Gem og afslut

Tryk på F10 (normalt) for at gemme og afslutte.

Bekræft ved at vælge Ja eller OK.

Computeren genstarter automatisk.

Trin 5: Installer BigLinux

Nu hvor Secure Boot er deaktiveret, kan du:

Starte normalt fra installations-USB-drevet.

Følge den normale BigLinux-installationsproces.

Vælge dit ønskede grafiske miljø (KDE, GNOME, Cinnamon eller Xfce).

Vigtigt: Den officielle BigLinux-wiki instruerer eksplicit brugerne i at deaktivere Secure Boot under installationen. Det er ikke færdigt endnu!

⚠️ Eksperimentelt alternativ: Brug Ventoy med Secure Boot

Advarsel: Denne metode understøttes eller testes ikke officielt af BigLinux. Brug på egen risiko!

Hvordan fungerer det?

Ventoy (et værktøj til at oprette multiboot-USB-drev) har en mekanisme til at arbejde med Secure Boot, hvor det installerer sit eget certifikat.

Trin-for-trin vejledning (eksperimentel)
Trin 1: Download og installer Ventoy

Gå til ventoy.net

Download Linux-versionen (eller Windows, hvis du foretrækker det)

Udpak filerne

Trin 2: Installer på et USB-drev med Secure Boot-understøttelse

I terminalen skal du navigere til Ventoy-mappen
cd ~/Downloads/ventoy-version/

# Kør med Secure Boot-indstillingen
sudo sh Ventoy2Disk.sh -s /dev/sdX

Erstat /dev/sdX med dit USB-drev (pas på ikke at vælge den forkerte disk!)

Trin 3: Kopier BigLinux ISO

Efter installationen vil USB-drevet have to partitioner

Kopier blot BigLinux ISO til den større partition (exFAT-format)

Trin 4: Registrer Ventoy-certifikatet (MOK)

Genstart computeren med USB-drevet tilsluttet

Start fra USB-drevet (bootmenu: F12, (F8 eller Esc)

Systemet vil gå ind i MOK (Maskinejernøgle) Administrationsværktøj.

Følg trinnene på skærmen:

Vælg “Tilmeld MOK”
Bekræft med “Fortsæt”
Indtast den ønskede adgangskode (normalt “ventoy” eller den, du har angivet)

Bekræft med “Genstart”

Trin 5: Initialiser BigLinux

Nu burde USB-drevet starte med sikker opstart aktiveret.

Vælg BigLinux ISO fra Ventoy menuen.

Systemet burde starte normalt.

⚠️ Kendte risici og begrænsninger

Risikobeskrivelse

Mangel på testning BigLinux tester ikke officielt denne metode. Ustabilitet Kan forårsage nedbrud eller tilfældige fejl.

Opdateringer Kernel/GRUB-opdateringer kan afbryde opstartsprocessen.

Drivere Proprietære drivere kan have problemer med sikker opstart.

Certifikat Nogle BIOS'er kan afvise Ventoy-certifikatet.

Windows Update Sikkerhedsopdateringer kan ugyldiggøre metoden.

📊 Sammenligning af muligheder

Udseende Deaktiver sikker opstart Brug Ventoy (eksperimentel)

Officiel support ✅ Ja ❌ Nej

Pålidelighed ✅ Høj ⚠️ Usikker

Kompleksitet ✅ Lav ⚠️ Mellem/Høj

Risiko for problemer ✅ Lav ⚠️ Moderat/Høj

Fremtidig vedligeholdelse ✅ Automatisk ⚠️ Kan kræve intervention

🎯 Endelig opsummering

Ven, her er det komplette svar på dit spørgsmål om BigLinux og Secure Boot:

Mulighed 1 - Anbefales (til alle):

Deaktiver Secure Boot i BIOS. Det er enkelt, hurtigt og garanteret. Følg den trinvise vejledning, jeg forklarede ovenfor. Uanset om du vil have KDE, GNOME, Cinnamon eller Xfce, er proceduren den samme og fungerer perfekt.

Mulighed 2 - Eksperimentel (kun for testere):

Hvis du virkelig har brug for at holde Secure Boot aktiv, kan du prøve Ventoy med certifikatregistrering (MOK). Vær dog opmærksom på, at:

BigLinux understøtter ikke denne konfiguration.

Du kan støde på uforudsigelige problemer.

Efter systemopdateringer kan det stoppe med at virke ud af ingenting.

Hvis du skal teste det, skal du sikkerhedskopiere dine data og være forberedt på at vende tilbage, hvis noget går galt.

Mit forslag: gå den sikre vej og deaktiver Secure Boot. Det tager kun et par klik i BIOS, og du vil sikre, at din BigLinux kører problemfrit uden fremtidige hovedpiner! 😉

Hej Snubbi! Jeg er glad for, at vejledningen var nyttig, og at du nu har et solidt fundament at vise din ven. Lad os dykke dybere ned i denne diskussion med teknisk information og en bredere kontekst om Secure Boot, fordi du berørte et afgørende punkt: de kommercielle og kontrolmæssige aspekter bag denne teknologi.

De reelle omkostninger ved "Trust Certificate"

Din opfattelse er helt korrekt. Processen for et operativsystem som BigLinux at blive genkendt af Secure Boot er ikke blot at "anmode om godkendelse" - det involverer betydelige omkostninger og tekniske barrierer, der fungerer som filtre på markedet.

Hvor meget koster det at signere en bootloader?

Baseret på teknisk dokumentation og community-rapporter:
Vare Omtrentlige prisdetaljer
EV Code Signing Certificate ~$2.000 (i 3 år) Dette er det specifikke certifikat, der kræves af Microsoft til at signere UEFI bootloadere. Det almindelige certifikat accepteres ikke.

Hardware-token Inkluderet i ovenstående pris. Leveres normalt på et fysisk USB-token (såsom SafeNet eToken), der indeholder den private nøgle.
Indsendelsesgebyrer Ikke eksplicit angivet, men der er administrative omkostninger. Processen kræver en Microsoft Partner Center-konto og overholdelse af snesevis af tekniske krav.
Ventetid Op til 6 måneder. Community-rapporter indikerer lange køer og bureaukratisk kommunikation med Microsoft.
Hardwarecertificering Yderligere gebyrer for producenter. Canonical (Ubuntu) opkræver for eksempel aktiveringsgebyrer for at certificere ikke-homologerede boards.
Den bureaukratiske proces

For at et projekt som BigLinux kan opnå Microsofts "segl", ville stien være:

Erhverv EV Code Signing-certifikatet fra en anerkendt certificeringsmyndighed (såsom DigiCert)
Sørg for, at bootloaderen er i PE/COFF-format (Microsoft-krav)
Implementer alle nødvendige sikkerhedspraksisser (ingen skrivbare/eksekverbare hukommelsesregioner osv.)
Indsend pakken til gennemgang fra Microsoft

Vent i måneder på et svar
Gentag processen med hver betydelig bootloader-opdatering

🔐 Kontroversen: Beskyttelse eller markedskontrol?

Den officielle diskurs

Secure Boot blev skabt som en del af UEFI-specifikationen for at beskytte mod bootkits - malware, der indlæses før operativsystemet og er praktisk talt usynlig for traditionel antivirussoftware. Mekanismen er teknisk neutral: den etablerer en tillidskæde, hvor hver komponent kryptografisk validerer den næste, før den udføres.

Den praktiske virkelighed

Problemet er ikke selve teknologien, men hvem der kontrollerer nøglerne, og hvordan denne kontrol udøves:

Nøglemonopol: Microsoft kræver, at pc-producenter med "Windows Certified"-seglet som standard inkluderer Microsoft-nøglen i UEFI. Det betyder, at Microsoft i praksis er blevet den globale certificeringsmyndighed for systemopstart.

Uoverkommelige omkostninger for små projekter: Mens store distributioner som Ubuntu, Fedora og Red Hat har råd til omkostningerne og bureaukratiet, er community-projekter som BigLinux, Manjaro og hundredvis af andre distributioner udelukket.

Kontrol over, hvad der "fortjener" tillid: Microsoft bestemmer, hvilke bootloadere der er "sikre" nok til at blive signeret - en enorm magt, der blander sikkerhed med kommercielle og tekniske kriterier, der ikke altid er gennemsigtige.

Begrænset gyldighed af signaturer: Nøgler har en udløbsdato. I september 2023 udløb en nøgle, der blev brugt af mange Linux-distributioner, hvilket krævede firmwareopdateringer, som producenterne ikke leverede til ældre modeller. De, der er afhængige af Microsofts infrastruktur, holdes som gidsler af denne tidsplan.

Hvad fællesskabet mener

Det frie softwarefællesskabs syn på Secure Boot er godt opsummeret i dette citat fra en teknisk Fedora-diskussion tilbage i 2012, men profetisk:

"Secure Boot i sig selv er bare et framework. Det siger, 'hey, hvis vi signerer alle disse bits, har vi en betroet boot-sti.' Det specificerer ikke, hvem der skal signere. Det er Windows 8-certificeringsprogrammet, der implementerer 'monopolkontrol' - det program, der kræver kompatibel hardware for at stole på Microsofts nøgle."

I nyere fora er tonen endnu mere kritisk:

"Hvis årsagen var sikkerhed ... er det ikke det, Secure Boot gør? Årsagen er ikke sikkerhed, årsagen er monopol."

🎯 Det virkelige problem: En "falsk følelse af sikkerhed"

Din vens argument om, at Secure Boot er "et beskyttelseslag", har teknisk værdi, men ignorerer den virkelige kontekst:

Selektiv beskyttelse: Secure Boot beskytter mod usigneret malware, men den beskytter ikke mod malware signeret af Microsoft eller nogen, den har tillid til. Hvis et ondsindet bootkit får en gyldig signatur (f.eks. gennem certifikattyveri), vil Secure Boot være fuldstændig ubrugelig.

Udelukkelse af legitime systemer: I mellemtiden behandles perfekt sikre systemer som BigLinux simpelthen som "ikke-tillid".