

**Klausimas.** NVR tech specifikacijos nurodyta, kad minimali HDD suma turi būti 60 TB, tačiau pasiūlymo formoje pildamoj lentelėj yra nurodyta, kad Tiekėjas turi pats parinkti tinkamą talpą ir pagrįsti.

Prašome atsakyti:

1. Kaip Tiekėjas turi tai pagrįsti? Kokius dokumentus pateikti?
2. Jei Tiekėjas pagrįs, kad reikia mažiau HDD talpos nei nurodomam minimaliam 60 TB, ar tai skaitysis, kad neprastesnis sprendinys?

Prašome pratęsti pasiūlymo pateikimo terminą iki 2026-06-17, nes dėl laiko zonų skirtumo ir gamintojų keliamų bei ruošiamų dokumentų užtrunka dokumentų kaip visumos surinkimas, bei tinkamo sprendinio ir pasiūlymo atlikimas.

**Atsakymas.** Perkančioji organizacija paaiškina, kad pirkimo dokumentuose nustatyti reikalavimai dėl vaizdo įrašymo įrenginio ir vaizdo įrašų saugyklos talpos turi būti vertinami kartu. Reikalavimas dėl ne mažesnės kaip 60 TB maksimalios bendros talpos apibrėžia vaizdo įrašymo įrenginio technines galimybes, o reikalavimas saugoti vaizdo įrašus ne trumpiau kaip 30 kalendorinių dienų – privalomą vaizdo įrašų saugojimo trukmę. Šie reikalavimai tarpusavyje neprieštarauja. Tiekėjas, įvertinęs siūlomą techninį sprendimą, turi pasiūlyti tokią saugyklos talpą ir ją pagrįsti skaičiavimu, kad būtų užtikrintas ne trumpesnis kaip 30 kalendorinių dienų vaizdo įrašų saugojimas. Atsižvelgiant į tai, pirkimo dokumentų sąlygos šiuo aspektu nekeičiamos. Tiekėjas privalo laikytis visų Techninės specifikacijos ir kitų pirkimo dokumentų reikalavimų.

**Klausimas.** Prašome panaikinti Tinklinis vaizdo įrašymo įrenginio tech. Specifikacijos reikalavimą „Secure boot“. Tiekėjas kaip rinkos lyderis ir savo srities profesionalas pareiškia, kad Perkančiajai organizacijai šis parametras nėra reikalingas, nes:

1. Tiekėjo siūlomas NVR Hanwha Vision XRN-3220RB2 naudoja Intel 12-os kartos platformą + TPM (Trusted Platform Module), o tai reiškia:

- įrenginys paleidžiamas su gamintojo pasirašytu firmware
  - naudojamas root-of-trust (TPM + UEFI/firmware chain)
  - paleidimo grandinė tikrina komponentų vientisumą automatiškai
2. TPM jau atlieka tą pačią funkciją
- Įrenginyje integruotas TPM:
  - tikrina firmware vientisumą
  - saugo kriptografinius raktus
  - užtikrina „measured boot“ principą

- Secure Boot funkcija dubliuotų TPM + firmware pasirašymo mechanizmą, todėl būtų perteklinė.

3. Secure Boot reikalingas, kai vartotojas gali keisti boot grandinę, tačiau Tiekėjo siūlomas įrenginys:

- neturi atviro BIOS/UEFI vartotojui
- neturi OS pakeitimo galimybės
- naudoja uždara embedded platformą

Todėl įvertinus Hanwha Vision XRN-3220RB2 architektūrą ir saugumo modelį, yra aišku, kad atskiro „Secure Boot“ parametro konfigūravimas nėra reikalingas.

**Atsakymas.** Nors Tiekėjo nurodytas įrenginys naudoja TPM ir pasirašytą firmware, pažymime, kad Secure Boot ir TPM atlieka skirtingas, viena kitą papildančias saugumo funkcijas: Secure Boot užtikrina neleistino kodo blokavimą paleidimo metu, o TPM leidžia įvertinti paleidimo grandinės vientisumą.

Todėl Secure Boot reikalavimas laikytinas papildoma saugumo priemone, o ne dubliuojančiu funkcionalumu.

Atsižvelgiant į tai, kad atsakymai į paklausimus teikiami likus mažiau nei 1 d. d. iki pasiūlymų pateikimo termino pabaigos – pasiūlymų pateikimo terminas yra pratęsiamas.

Pasiūlymų pateikimo terminas – 2026 m. birželio 17 d.

Paklausimų ir paaiškinimų pateikimo terminas nebepratęsiamas.