

**Solicitare clarificari procedura nr. 5635/09.12.2021- Servere pentru
infrastructură de virtualizare**

Solicitare Clarificare:

Va rugam sa eliminati urmatoare cerinta , atat la server de tip 1 cat si la server de tip 2:

“Firmware -Mecanism de protectie a firmware-ului pe baza amprentei hardware , oprind secventa de boot in cazul in care se constata modificari ale configuratiei”

Creдем ca exista o confuzie intre posibilitatea de a scrie firmware nesemnlat criptografic si capacitatea de a opri secventa de boot in cazul modifica configuratia sistemului.

Aceste doua componente sunt complet separate intre ele.Capabilitatea de a modifica configuratia sistemului se coreleaza cu liste de roluri si permisiuni (ACL) nu cu mecanismul de protectie criptografic de la nivelul firmware-ului.

Răspuns clarificare:

Echipamentele ofertate trebuie sa implementeze mecanisme precum Intel Boot Guard.