TARTU ÜLIKOOL
Arvutiteaduse instituut
Informaatika õppekava

Keity Raudmäe

Operatsioonisüsteemi Windowsi 11 standardsed riistvara turbetehnoloogiad ja nende turvaline kasutamine HP Elitebook 840 G8 näitel

Bakalaureusetöö (9 EAP)

Juhendaja: Alo Peets

Tartu 2022

Operatsioonisüsteemi Windowsi 11 standardsed riistvara turbetehnoloogiad ja nende turvaline kasutamine HP Elitebook 840 G8 näitel

Lühikokkuvõte:

Käesoleva töö eesmärk on luua eestikeelne materjal tänapäevastest standardsetest riistvara turbetehnoloogiatest, mis Microsoft Corporationi uue Windows 11 operatsioonisüsteemiga on päevakorda kerkinud. Töös kirjeldatakse turbetehnoloogiaid nagu turbeprotessor, turvaline käivitus ning virtualiseerimispõhine turvalisus. Nendest turbelahendustest tulenevalt on täpsemalt kirjeldatud turbeprotsessoriga seotud Windowsi turbefunktsioone BitLocker ning Windows Hello. Lisaks eestikeelsele materjalile on töö üheks väljundiks riistvaraliste turbelahenduste praktiline testimine Windows 11 operatsioonisüsteemis ning HP Elitebook 840 G8 seadmel.

Töö teoreetilise osa tulemuseks on turbetehnoloogiatest eestikeelne materjal, millele on võimalik lugejal oma töös vajadusel toetuda. Praktilise osa tulemusena tõdeti, et HP Elitebook 840 G8 seadmel on tootja poolt turbetehnoloogiate kasutamine tehtud mugavaks ja kasutajast sõltumatuks. Lisaks järeldati, et Windows 11 turbelahendused on kasutatavad ka operatsioonisüsteemis Windows 10, kui seade vastab turbetehnoloogiate nõuetele.

Võtmesõnad:

Windows 11, turbeprotsessor, turvaline käivitus, virtualiseerimispõhine turvalisus

CERCS: P175, Informaatika, süsteemiteooria

Windows 11 standard hardware security technologies and their secure usage based on HP Elitebook 840 G8

Abstract:

The aim of this research is to create Estonian-language material about modern standard hardware security technologies which Microsoft Corporation has made topical with their new operating system Windows 11. The paper describes security technologies such as trusted platform module (TPM), secure boot and virtualization-based security. TPM related Windows security features like BitLocker and Windows Hello are also described. In addition to Estonian-language material one of the outputs of this work is the practical use of these security solutions in Windows 11 operating system and the HP Elitebook 840 G8 device.

The outcome of this research's theoretical part is the Estonian-language material for the aforementioned modern standard hardware security technologies to which the reader can refer to in their future work if needed. As a result of the practical part of this research it was found that the use of security technologies on the device of HP Elitebook 840 G8 is made more convenient and user independent by the manufacturer. In addition, it was concluded that the hardware security technologies in Windows 11 are also present in Windows 10, if the device meets the hardware requirements.

Keywords:

Windows 11, TPM, secure boot, virtualization-based security

CERCS: P175, Informatics, systems theory

Sisukord

Sissejuhatus

Üks enim kasutatud operatsioonisüsteeme on juba personaalarvutite algusaegadest Microsoft Corporation'i kaubamärk Windows, mis on 2022 aasta jaanuari seisuga Euroopas kõige populaarsem operatsioonisüsteem, omades turuosast pea 78% [1]. Kõige uuem operatsioonisüsteem Windows 11, mis tehti avalikkusele kättesaadavaks 5. oktoober 2021, sai ootamatult karmide süsteeminõuetega juba enne turule tulemist omajagu kriitikat [2-5]. Võttes aluseks Microsofti turbeteenuse materjalid [6], on Windows 11 turvalisus üles ehitatud täisusaldamatuse turbepoliitikal. Täisusaldamatus tähendab seda, et igal ajahetkel, ükskõik kus, võib süsteem olla ära kasutatav. Sellest tulenevalt ei tohi ühtegi süsteemi kasutamise komponenti pidada usaldusväärseks ning rakendatakse järgnevalt välja toodud põhimõtteid. Esiteks enne juurdepääsude andmist tuleb kõik juurdepääsutaotlused autentida, autoriseerida ja krüpteerida. Teiseks on oluline külgrünnete ennetamine ja seetõttu tuleb rakendada mikrosegmentimise ja vähimate eelisõigustega juurdepääsu põhimõtteid. Kolmandaks kasutatakse anomaaliatele reageerimiseks reaalajas mitmekülgseid tuvastus- ja analüüsifunktsioone.

Selleks, et täisusaldamatuse turbepoliitikat reaalselt rakendada, on Microsoft [7] uuele operatsioonisüsteemile seadnud resoluutsed riistvaraturbe nõuded:

1) usaldatava platvormi mooduli (edaspidi turbeprotsessor või TPM) versioon peab olema 2.0;
2) süsteemi püsivara peab toetama UEFI turvalist käivitust;
3) kahe või rohkema tuumaline vähemalt 1 GHz kiirusega protsessor peab kasutama kaasaegseid draivereid ja toetama virtualiseerimise liideseid.

Seega on Microsofti uue operatsioonisüsteemiga päevakorda kerkinud riistvaralised tehnoloogiad, millest tavakasutajal teadmised on puudulikud või puuduvad täiesti. Lisaks eestikeelset materjali, mis sisaldaks just neid Windows 11 riistvara turbenõuetest tulenevaid turbelahenduste ja -tehnoloogiate kirjeldust, on vähe või puudub selle alane kirjandus üldse. Windows 11 on miinimumnõuded muuhulgas ka graafika kaardile, ekraanile ning muutmälule, kuid need pole turvastandarditega otseses seoses ja neid selle töö raames ei käsitleta. Kogu operatsioonisüsteemi Windows 11 nõuete nimekiri on leitav Microsofti veebilehelt[1].

Eestis on üleüldine küberkuritegude arv pidevas kasvutrendis [8]. Seega on erinevate turbetehnoloogiate areng tavakasutaja jaoks oluline, sest pidevalt arenevas infotehnoloogia valdkonnas leitakse ikka ja jälle erinevaid turvanõrkusi [9] ning kasutajatelt andmete õngitsemismeetodid on järjest usutavamad ning personaalsemad, muutes igasuguse süsteemi haavatavaks lunavararünnete vastu. Kuna ka operatsioonisüsteemide ja antiviiruse tarkvara tarnijad karmistavad oma koodi, muudavad ka pahavara arendajad oma strateegiaid pidevalt – võetakse sihiks rünnata alglaadimise eelset keskkonda [10]. Selliste rünnete puhul kerkivad päevakorda seadme riistvaralised turbelahendused.

Bakalaureusetöö üheks eesmärgiks on anda eestikeelne ülevaade tänapäevastest riistvaralistest turbelahendustest nagu seda on turbeprotsessor, visualiseerimispõhine turvalisus ning turvaline käivitus. Töö teoreetiline osa katab mainitud turbetehnoloogiate tööpõhimõtete kirjeldust ning

osadel juhtudel ka konkreetsemaid näiteid (BitLocker, Windows Hello). Töö teise osa eesmärk on vaadelda ja kirjeldada turbetehnoloogiate praktilist kasutust operatsioonisüsteemis Windows 11 seadmel HP EliteBook 840 G8, mis on töö kirjutamise hetkel Tartu Ülikooli arvutiteaduste instituudis tudengitele õpingute ajaks pakutav kõige uuem sülearvuti. Lisaks võrreldakse praktilises osas tehnoloogiaid Microsofti varasema operatsioonisüsteemi Windows 10-ga. Tulemuseks on kokkuvõttev materjal, mille põhjal saab Windowsi tavakasutaja teha teadlikke otsuseid seoses seadmete ja nendega seotud turbetehnoloogiatega. Kuna töö katab vaid väikese osa kõikidest Windowsi turvalisusega seotud funktsioonidest, siis on see sobiv alus edasiseks uurimistööks ja analüüsiks.

Töö koosneb kuuest peatükist, kokkuvõttest ning lisadest. Esiteks on välja toodud mõisted ja terminid, mille eesmärk on anda põhjalik ülevaade esinevatest mõistetest ja seda ennekõike informaatika sõnavaraga mitte kursis olevale lugejale. Teadjamad lugejad võivad esialgu peatüki vahele jätta ning vajadusel materjali läbides selle juurde tagasi tulla. Esimeses sisulises peatükis antakse ülevaade turbeprotsessorist, selle alamosades kirjeldatakse operatsioonisüsteemi Windowsi ning turbeprotsessori kasutusvõimalusi. Lisaks on selles peatükis kaetud ka Windowsi turbelahendused - kasutaja autentimise raamistik Windows Hello ning ketta krüpteerimise tehnoloogia BitLocker. Teises peatükis kirjeldatakse UEFI turvalise käivituse tehnoloogiat. Kolmas peatükk sisaldab virtualiseerimispõhise turvalisuse tehnoloogilisi lahendusi – mälu terviklus ning protsessori mudelipõhiste registrite kaitset. Testitava seadme HP Elitebook 840 G8 tehnilise ülevaate leiab neljandast peatükist. Turbetehnoloogiate praktiline kasutus on kirjeldatud peatükis number viis ning praktilise kasutuse põhjal tehtud järeldused leiab peatükist number kuus. Lisad sisaldavad erinevate turbefunktsionaalsustega seotud taustandmeid ning seadistamise juhiseid.

[1] www.microsoft.com/en-us/windows/windows-11-specifications

Mõisted ja terminid

Ainulogimisega pöördus - *Single sign-on access*; lühend SSO; pääsu reguleerimise funktsioon, mis võimaldab kasutajal pöörduda üheainsa sisselogimisega paljude eri ressursside poole[2]

Atesteerimisvõti - *attestation identity key*; krüptoprotsessoris TPM resideeriv RSA-võti platvormi autentimiseks[2]

Buutkratt - *bootkit*; juurkrati kõrgem vorm, suudab nakatada üldbuutkirje MBR või sektsiooni buutkirje[2]

CBC-tööviis - *cipher-block chaining mode*; krüptogrammiplokkide aheldusega tööviis, mis on üks plokkšifri tööviise[2]

CTAP - *Client to Authenticator Protocol*; kliendi autentimisprotokoll[3]

Deklaratiivse, komponentseeritud, riistvara tugirakenduste nõuetele vastav - *DCH- compliant (Declarative, Componentized, Hardware Support Apps)*[3]

DMA - *direct memory access*; otsemällupöördus on meetod andmete teisalduseks otse põhimälu ja välisseadmete vahel, nõudmata protsessorilt andmete töötlust[2]

Draiver - *driver*; draiver on seadme juhtprogramm, mis liidestab tarkvara riistvaraga[2]

FIDO2 - *Fast IDentity Online*; onlain-kiiridentiteet, mis on paroolivaba lahendus FIDO U2F lahendusest[2]

HVCI - *Hypervisor-protected Code Integrity*; Windowsi virtualiseerimisel põhineva turvalisuse funktsioon[3]

Hübriidtuum - NTOS kernel; Windows NT kernel; tuum, mis on vastutav seadme draiverite initsialiseerimisel alglaadimisel[4]

Identiteeditarnija - *identity provider*; usaldatav teenuseandja, kes loob, haldab ja autendib kasutajate identiteete[2]

IP-aadress - IP võrku (TCP/IP võrku) ühendatud arvuti või muu seadme identifikaator[5]

Juurkratt - *rootkit*; juurkasutaja õigustega kahjurvara[2]

Kaheastmeline kinnitamine - *two-step verification*; ka topelt kontroll on kahe autentimismeetodi järjestikku rakendamine[2]

Kahjuritõrje tarkvara - *Anti-malware software*; tarkvara, millega välditakse, avastatakse ja kõrvaldatakse paljusid kahjurvara liike[2]

Klahvinuhk - *keylogger*; nuhkvara, mis talletab salaja kasutaja klahvivajutusi ja ka muid sisestustoiminguid[2]

Külgrünne - *lateral movement*; rünne, mille lähte- ja sihtkoht on samas võrgus[2]

Lehekülg – *page*; *paging* virtuaalmälusüsteemides kujutab lehekülg endast kindlat baitide arvu, mida operatsioonisüsteem käsitleb ühe tervikuna[5]

Lüüs - *gateway*; funktsionaalüksus, mis ühendab kaht arhitektuurilt üksteisest erinevat arvutivõrku[2]

MAC-aadress - meediumipöörduse juhtimise aadress, kohtvõrgus (või mõnes muus võrgus) on MAC-aadress arvuti võrgukaardile tootja poolt omistatud unikaalne riistvaranumber[5]

Mahtuvuslik sõrmejälje sensor - *capacitive fingerprint sensor*; vedelkirstall-ekraani ette on paigutatud veel üks klaas, mille tagaküljele on kantud läbipaistvast elektrit juhtivast materjalist kile[2]

Mikrosegmentimine - *microsegmentation*; võrgu turvatehnoloogia, mis võimaldab turvaarhitektidel jagada andmekeskus loogiliselt eraldiseisvateks turbesegmentideks, määratledes turvakontrollid ning pakkudes teenuseid iga unikaalse segmendi jaoks[3]

Originaalseadmete tootja - *Original Equipment Manufacturer*; lühend OEM; selles töös kasutusel uuem tähendus ehk firma, kes ostab teise firma toote ja paigutab selle oma tootesse või muudab uueks tooteks oma kaubamärgi all[2]

Parandusmeede - *remediation*; nõrkuse või ohu kaotamine, kõrvaldamine[2]

PIN - *personal identification number*; isiku identifitseerimisnumber, lühike parool[2]

Progressiivne krüpteerimisstandard - *Advanced Encryption Standard*; lühend AES progressiivne krüpteerimisstandard, mis on sümmeetrilise võtmega plokkšiffer[2]

Püsivara - *firmware*; püsivara on programmikoodi või andmeid sisaldav riistvara, mille sisu ei saa lõppkasutaja keskkonnas muuta[2]

Rikkumiskindel – *tamper resistant;* kaitse passiivse füüsilise ründe eest[2]

Räsi – *hash;* väärtus või bitijada, mis on andmetest saadud räsifunktsiooni abil ühesuunalise krüpteerimisega[2]

Serverimurre - *server breach*; turvanõrkuse tekitamine serveris[2]

Signatuurandmebaas - *signature database*; struktureeritud signatuuri kogumite komplektid, mida kasutatakse kas tuvastusalgoritmide hindamiseks või operatsioonisüsteemi osana[6]

Signeerima - *sign*; infoturbes, signatuuri genereerimise protsess, mis kasutab signatuuri loomiseks sõnumit ja signeerija signeerimisvõtit[2]

Sõnastikrünne - *dictionary attack*; jõuründe liik, mille puhul parooli või muu saladuse mõistatamiseks proovitakse suurest loendist võetud sõnu või sõnakombinatsioone[2]

Säilmälu - *non-volatile memory*; lühend NV-RAM; toite kadumisel oma sisu säilitav mäluliik[2]

Taasesitusrünne - *replay attack*; rünne, mis põhineb pealtkuulamisega saadud andmete salvestusel ja samale vastuvõtjale saatmisel[2]

Taastevõti - *recovery key*; loogiline omanikuvõti, lukustunud seadme vabastamiseks seadmest sõltuvas tähenduses[2]

Teesklustõrje - *anti-spoof*; meetmed teeskluse tõkestamiseks[2]

Terviklus - *integrity*; andmete õigsus, täielikkus, kooskõla[2]

Turbeprotsessor - *Trusted Platform Module*; lühend TPM; usaldatava või usaldusväärse platvormi moodul, krüptoprotsessor, mis on spetsialiseeritud kontrollerkiibina ning toetab selle tehnilises spetsifikatsioonis kirjeldatud tehnoloogiaid (nagu võtmete genereerimine, krüpteerimine)[2,4]

Turvaline käivitus - *Secure Boot*; ühtse laiendatava püsivaraliidese funktsioon[4]

Täisusaldamatuse turbepoliitika - *Zero Trust policy*[3]

UEFI põhivara draiverid - *Option ROM and UEFI firmware drivers*[3]

Usaldatav andmetöötlusplatvorm - *Trusted Computing platform*; usaldatava andmetöötluse tehnoloogial põhinev riistvara koos kompilaatoriga, millele rajatakse tegelik süsteem[2,3]

Usaldatava platvormi moodul – vaata mõistet „Turbeprotsessor“

Usaldatav täitmiskeskkond - *trusted execution environment*; lühend TEE; turvaline keskkond tundlike andmete töötluseks, mis on harilikust täitmiskeskkonnast lahutatud eraldi protsessorialal[2]

Viseerimisvõti - *endorsement key*; Trusted Computing süsteemis kasutatav RSA-krüpteerimisvõti[2]

Värkvõrk - *internet of things;* lühend IoT; Interneti pealisvõrk nutiseadmete ühendamiseks[2]

Vääreitustegur - *false reject rate*; lühend FRR; väite ekslike vääraks tunnistamiste osakaal[2]

Väärjaatustegur - *false accept rate*; lühend FAR; väite ekslike tõeseks tunnistamiste osakaal[2]

Windowsi taastamise keskkond - *Windows Recovery Environment*[4]

Windwowsi alglaadimishaldur - *Windows Boot Manager*[4]

Õngitsema - *phishing*; teesklus, mille sooritaja saadab tundliku teabe saamiseks sõnumeid, mis näivad tulevat erinevatest suhtluskanalitest[2]

Ühtne laiendatav püsivaraliides - *Unified Extensible Firmware Interface*, lühend UEFI, püsivara ja operatsioonisüsteemi vahelise buutliidese spetsifikatsioon, asendab BIOSi[2]

XTS-AES krüpteerimismeetod - *XEX tweakable block ciphertext stealing*; XTS põhineb “šifreeritud teksti varastamise” meetodil, millega saab krüpteerida ja dekrüpteerida suvalise pikkusega andmeploki jadasid[7]

---

[2] https://akit.cyber.ee/
[3] https://doubleoctopus.com/security-wiki/
[4] https://www.microsoft.com/et-ee/
[5] http://www.vallaste.ee/
[6] https://link.springer.com/
[7] https://xilinx.github.io/

1 Turbeprotsessor

Turbeprotsessor on pea igas kaasaegses seadmesse sisse ehitatud. Selle eesmärk on võimaldada süsteemi platvormile erinevaid turbefunktsioone, tagades seeläbi seadmele kõrgendatud turvalisuse. Turbeprotsessor on seadmes füüsiline kontrollerkiip, mis toetab erinevaid krüptotehnoloogiaid, muuhulgas võtmete genereerimist ja krüpteerimist. Eesti keeles pole turbeprotsessori mõiste laialt levinud, sest otsetõlkes on selle täpne vaste usaldatav (või usaldusväärne) platvormi moodul. Kuna keeleliselt on turbeprotsessori mõiste aga lühem ja mugavam ning ka Microsofti eestikeelses dokumentatsioonis on kasutusel mõiste „Turbeprotsessor“, siis edaspidi kasutatakse antud töös just seda.

Selleks, et seade vastaks operatsioonisüsteemi Windows 11 nõuetele on esimeseks oluliseks turbetehnoloogiaks turbeprotsessori olemasolu ning täpsemalt versioon 2.0. See peatükk tutvustab turbeprotsessori olemust ning selle kasutusvõimekust. Lisaks on välja toodud nimekiri Windowsi funktsioonidest, mis kasutavad turbeprotsessorit ning vaadeldakse väga konkreetseid tavakasutaja jaoks olulisi lahendusi nagu Windows Hello ning BitLockeri ketta krüpteerimine.

TPM on ISO/IEC 11889-1:2015 standardi[8] järgi kirjeldatud kui seade, mis võimaldab turvalisi seoseid erinevatel andmetöötlus platvormidel. Selle looja ja haldaja on mittetulunduslik organisatsioon The Trusted Computing Group (TCG). TCG avaldab nõuded turbeprotsessorile rahvusvahelises ISO/IEC 11889-1:2015 [11] standardis. Viimane standardi ülevaatus toimus 2021 aastal ja järgmine planeeritud ülevaatus toimub 2025 aastal.

TCG annab oma artiklis “TPM 2.0 A Brief Introduction” [12] ülevaate turbeprotsessorite eri tüüpidest, mis olenevalt kasutusvaldkonnast, on järgmised:

1) Virtuaalne TPM, mis on tavapäraselt kasutusel pilvekeskkondades. Värkvõrkudes (IoT), kus kasutatakse virtualiseerimist, on virtuaalne TPM osa pilvepõhisest keskkonnast ning võimaldab igal eraldiseisval virtuaalmasinal kasutada samu käske, mis füüsiline TPM.
2) Tarkvara TPM on tavapäraselt kasutusel testimises ja prototüüpimises. See simuleerib füüsilise turbeprotsessori funktsionaalsust, olles seejuures tarkvaraliste turvaaukude tõttu haavatav. Seetõttu kasutatakse tarkvara turbeprotsessorit ennekõike turbeprotsessoritega süsteemide testimiseks ja prototüüpimiseks.
3) Põhivara TPM on kasutusel enamasti meelelahutussüsteemides. Põhivara turbeprotsessor luuakse kaitstud tarkvaras. Kood töötab seadme põhiprotsessoril, seega eraldi kiip ei ole vajalik. Kuna ta töötab nagu iga teine programm, siis kood töötab usaldatavas täitmiskeskkonnas (TEE), mis on eraldatud teistest protsessori programmidest. Põhivara TPM turvalisus sõltub paljudest erinevatest osadest, nagu operatsioonisüsteem ja vead TEE koodis, muutes selle ebasobivaks kriitiliste süsteemide jaoks.
4) Integreeritud TPM on riistvaraline turbeprotsessor, mis on eraldi integreeritud kiibile. Selle eesmärk on anda edasi rohkem turbeprotsessori funktsionaalsust kui turvalisust.

Riistvaraline lahendus teeb selle tarkvaraliste rünnete suhtes turvaliseks, kuid mitte rikkumiskindlaks. Tavapäraselt on kasutusel lüüsides.

5) Diskreetne TPM on kasutusel kriitilistes süsteemides ning kõige kõrgemat turvalisust vajavates seadmetes. Selle eesmärk on tagada, et süsteemi ei ole võimalik ka kõige keerulisemate meetoditega rünnata. Selle tagamiseks kasutatakse diskreetse turbeprotsessori arendamisel kõige kõrgemat turvataseme hindamist, mis suudab kiibi rikkumist takistada kõikvõimalike keerulisemate rünnakute eest.

Microsofti artikli "TPM recommendations" [13] järgi on kõige tavalisem turbeprotsessori tüüp diskreetne TPM, et OEM ehk originaalseadmete tootja saaks turbeprotsessorit eraldiseisvalt hinnata. See aga ei sobi integreeritud seadmetesse, mis on väiksed ja vähese voolutarbimisega. Uuemad lahendused integreerivad turbeprotsessori funktsionaalsuse samale kiibistikule, kus ülejäänud süsteemi osad. Sarnaselt diskreetsele turbeprotsessorile tagatakse siiski loogiline erisus. Microsofti enda operatsioonisüsteem Windows kasutab kõiki ühilduvaid turbeprotsessoreid olenemata tüübist ühtemoodi.

Microsoft, kes on ka TCG liige, väidab [7] turbeprotsessori kohta järgmist: "TPM on arendatud odava massturu turvalahendusena, mis vastaks erinevate kliendisegmentide nõuetele." Arvutites on tavapäraselt TPM otse seadme emaplaadile paigaldatud spetsialiseeritud kontrollerkiip, mis kasutab ülejäänud süsteemiga suhtlemiseks riistvara siini. Seda selleks, et masina originaalseadmete tootja saaks hinnata ja kinnitada turbeprotsessorit ülejäänud süsteemist eraldi. Microsofti materjalidest [14] lähtudes kasutab turbeprotsessor enda sisemist püsivara ja loogikalülitusi, et töödelda saadavaid käske. Kuna TPM ei ole operatsioonisüsteemist sõltuv, ei ole see haavatav erinevatele turvanõrkustele, mis on operatsioonisüsteemis endas või rakenduste tarkvaras.

TPM arendatakse originaalseadmete tootja poolt osana usaldatavast andmetöötlusplatvormist. Selleks võib olla näiteks personaalarvuti, tahvelarvuti või telefon. TPM kasutusvaldkond laieneb aga ka mujale. TCG väljaande [12] kohaselt rakendatakse turbeprotsessorit ka autodes, tööstustes, nutikodudes ja paljudes teistes rakendusvaldkondades. Usaldatavatel andmetöötlusplatvormidel on vajalik TPM selleks, et toetada privaatseid ja turvalisi stsenaariumeid, mida ainuüksi tarkvaraliselt ei ole võimalik saavutada.

Toetudes Microsofti materjalidele [13] loodi TPM algselt selleks, et tagada platvormi omanikule ja kasutajatele turvalist ning privaatset süsteemi kasutust. Uuemad versioonid tagavad samad omadused süsteemi riistvarale endale. Turbeprotsessoril on palju erinevaid funktsionaalsusi. TPM 2.0 on üle võtnud kõik TPM 1.2 olevad funktsionaalsused ning lisaks on parendatud vanu ja arendatud uusi. Võttes aluseks raamatu "A Practical Guide to TPM 2.0" [15] on välja toodud põhilised TPM 1.2 võimalused:

1) Seadmete tuvastamine turvatunnuse alusel - enne turbeprotsessori loomist oli seadme tuvastamise aluseks IP või MAC-aadress.

2) Turvaline võtmete genereerimine - riistvaraline suvalise numbri genereerimine on suureks eeliseks, sest nõrga võtme genereerimise tõttu on paljud turvalahendused manipuleeritavad.

3) Turvaline võtmete hoiustamine - kuna turbeprotsessor on eraldiseisev riistvaraline siin, siis on võtmed seal tarkvaraliste rünnakute eest kaitstud.

4) Säilmälu hoiustamine - säilmälu olemasolust tulenevalt on turbeprotsessoril võimekus omada sertifikaadiladu.

5) Seadme tervisetõend - süsteemi heaolu kindlaks tegemisel on varasemalt kasutatud tarkvaralisi lahendusi, mis võisid anda valeinfot süsteemi tervise kohta.

Lisaks TPM 1.2 funktsionaalsustele on versioonis 2.0 olemas järgnevad funktsionaalsused:

6) Algoritmide võimekus - kui selgub, et krüptograafiliselt on algoritm nõrgem kui vaja, saab algoritme muuta ilma nõudeid muutmata.

7) Täiendatud autoriseerimine - uus versioon ühtlustas selle, kuidas üksuseid turbeprotsessoris autoriseeriti. Nüüd lubatakse ka autoriseerimine mitme teguri ja mitme kasutaja vahel. Samuti lisati haldusfunktsioone.

8) Võtmete kiire laadimine - võtmete laadimine võttis eelnevas versioonis palju aega. Sümmeetrilise krüpteerimise abil saab TPM 2.0 võtmeid kiiresti laadida. Varasemalt oli kasutusel asümmeetriline laadimine.

9) Turbeprotsessori eelnevas versioonis esines halduspробleeme, kui võtmeid lukustati seadme olekusse. Kui seadme olek vajas autoriseeritud oleku muutust, vajasid ka võtmed muutmist. TPM 2.0 seda probleemi enam ei esine.

10) Paindlik haldus - erinevad autoriseerimised on üksteisest eraldi, mis võimaldavad turbeprotsessori ressurssi paindlikult hallata.

11) Nime järgi identifitseeritud ressursid - turbeprotsessori varasemas versioonis olid viited ebatäpselt disainitud, mis põhjustasid erinevaid turvalisuse alaseid väljakutseid. TPM 2.0 versioonis on kõikidele TPM ressurssidele pandud krüptograafiliselt turvalised nimed.

Kuna turbeprotsessoril on väga palju erinevat funktsionaalsust ning sellest tulenevaid kasutusvaldkondi, siis antud töö on piiratud Windowsi poolt kasutatud turbeprotsessori funktsionaalsustega.

1.1 Windows ja turbeprotsessor

Lähtudes Windowsi dokumentatsioonist “Trusted Platform Module 2.0” [16], on alates operatsioonisüsteemidest Windows 10 ja Windows 11 turbeprotsessori omaniku õigused ja lähtestamine automaatselt operatsioonisüsteemi kanda. Sisuliselt tähendab see seda, et seadme omanik ei pea enam turbeprotsessorit seadistama ega jälgima. Süsteemi kasutajal on see võimalus siiski olemas. Microsoft oma dokumentatsioonis [17] aga soovitab vältida turbeprotsessori seadistamist TPM halduskonsooli (TPM.msc) kaudu. Eranditeks on seadmele operatsioonisüsteemi uuesti paigaldamine (puhas install) või seadme lähtestamine. TPM kasutuseelistena on Microsoft [17] välja toonud järgmised funktsionaalsused:

1) krüptovõtmete genereerimine, hoiustamine ning kasutusvõimaluste piiramine;

2) TPM tehnoloogia, mis võimaldab kasutada seadme autentimiseks turbeprotsessorisse endas hoiustatud unikaalset RSA võtit;

3) platvormi tervikluse tagamine.

Kõige tavapärasemalt kasutatakse turbeprotsessori funktsioone süsteemi tervikluse kontrollimiseks ning võtmete genereerimiseks ja kasutamiseks.

Windowsi "TPM fundamentals" [14] ütleb, et arvutid, milles on TPM, suudavad luua krüptograafilisi võtmeid ja krüpteerida neid nii, et neid saab dekrüpteerida kasutades vaid turbeprotsessorit ennast. Selline võtme sidumise protsess aitab kaitsta võtit avalikustamise eest. Iga TPM omab üldvõtit, mida kutsutakse juurvõtmeks ning seda hoiustatakse turbeprotsessoris endas. Juurvõtme privaatne osa on loodud turbeprotsessoris ning seda ei avalikustata ühelegi teisele komponendile, tarkvarale, protsessile või kasutajale. Krüpteerimisvõtmeid saab migreerida, mis tähendab, et krüpteerimisvõtme üks avalik või privaatne osa on avalikustatud mõnele komponendile, tarkvarale, protsessile või kasutajale.

Võttes aluseks Microsofti dokumentatsiooni "How Windows uses the Trusted Platform Module" [18] saab välja tuua järgmised Windowsi funktsionaalsused, mis kasutavad turbeprotsessorit:

1) Platvormi krüptoteenuse pakkuja on Windowsi krüptograafiline API raamistik arendajatele. See kasutab turbeprotsessorit võtmete loomiseks, nende kaitsmiseks ning sõnastikrünnete kaitseks. Nii Windows ise (Windows Hello autentimisteenus) kui ka kolmanda osapoole rakendused saavad kasutada API raamistikku ilma ise krüpteerimiseks mõeldud keerulisi algoritme arendamata.

2) Virtuaalse kiipkaardi funktsionaalsus kasutab turbeprotsessorit kiipkaardi ajutiseks matkimiseks. Virtuaalse kiipkaardi kontekstis on turbeprotsessor midagi, mis kasutajal on olemas ja see nõuab midagi, mida kasutaja teab (PIN). Sarnaselt reaalse kiipkaardiga, on turbeprotsessoril funktsionaalsus sõnastikrünnete kaitseks. Sisuliselt piirab turbeprotsessor PIN-i valesti sisestamise kordade arvu. See funktsionaalsus on mõeldud organisatsioonidele, kes tahavad odavat ja mugavat, kuid samal ajal ka turvalist, autentimisteenust.

3) Kontrollitud alglaadimine (*Measured Boot*) on funktsionaalsus, mis salvestab operatsioonisüsteemi tarkvara komponentide ja algseadete näitajate (nagu Windowsi kernel, varajase käivituse viirusetõrje tarkvara draiverid, alglaadimise draiverid) ahela kasutades selleks turbeprotsessorit. Kontrollitud alglaadimine aitab leida pahavara juba alglaadimise protsessist alates. Kontrollimise infot on võimalik jagada välistele üksustele, et kinnitada seadme turbepoliitikate vastavust ning tõestada, et seade ei käivitunud koos pahavaraga. Windowsi operatsioonisüsteemides on kontrollitud alglaadimine alates operatsioonisüsteemist Windows 8.

4) Tervisetõend (*Health Attestation*) on teenus, mis loob erinevate turbeprotsessorite tootjate atesteerimisvõtme sertifikaadid. Lisaks on teenusel funktsionaalsus, mis kontrollitud alglaadimise tulemused töötleb lihtsaks turvalisusega seotud väiteks - näiteks kas BitLocker on sisse lülitatud või mitte. See on mõeldud ennekõike mobiilsete seadmete halduse (MDM) kaugseire jaoks organisatsioonides [19].

5) Mandaatide valvur (*Credential Guard*) on Windowsi funktsioon, mis aitab kaitsta Windowsi mandaate organisatsioonides, mis kasutavad Active Directory domeeniteenuseid. Mandaatide valvur kasutab virtualiseerimist, et hoida mandaadid eraldi ülejäänud süsteemist. Mandaatide kaitsmiseks kasutatakse turbeprotsessorit.

6) Windows Hello on funktsionaalsus, mille eesmärk on asendada lihtsasti ohtu seatavad ja raskesti meelde jäävad paroolid. Turbeprotsessorit kasutatakse Windows Hello raamistikus autentimises kasutatavate privaatsete võtmete loomiseks, kaitsmiseks ning hoiustamiseks.

7) BitLockeri ketta krüpteerimine (*BitLocker Drive Encryption*) ning BitLockeri seadme krüpteerimine (*BitLocker Device Encryption*) on Windowsi funktsionaalsused kõvaketta erinevate loogiliste jaotiste krüpteerimiseks. Tavapäraselt krüpteeritakse operatsioonisüsteemi jaotis. Seda selleks, et kui ketas või seade on kadunud või varastatud, siis jaotises olevad andmed jäävad konfidentsiaalseks. Täpsemalt on seos turbeprotsessoriga lahti seletatud eraldi alapeatükis. *Device Encryption* on tavakasutaja versioon BitLockeri ketta krüpteerimise funktsionaalsusest.

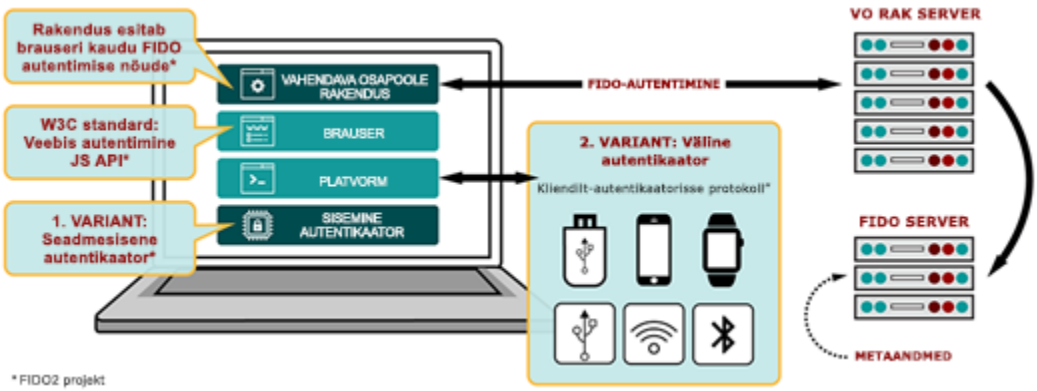
Suurem osa eespool mainitud funktsionaalsust on suunitlusega organisatsioonidele. Antud töös aga keskendutakse tavakasutaja jaoks olulisele kahele turbelahendusele. Esiteks Windows Hello, mis on kasutajate seas väga populaarne [20] ning teiseks eelseadistatud ning sisse lülitatud funktsionaalsus BitLockeri seadme krüpteerimine [21].

1.2 Windows Hello

Microsofti dokumentatsiooni [22] järgi esindab Windows Hello raamistiku, mis laseb kasutajal sisse logida seadmesse ja rakendustesse, kasutades selleks biomeetriat või PIN-i. Samal ajal ladustatakse turvaliselt kasutajanimi ja parool, lubades neid kasutada vaid siis, kui kasutaja identifitseerib end. Windows Hello raamistik on Microsofti poolne lahendus FIDO2 autentimisest, mis on alternatiiv paroolipõhisele autentimisele. FIDO2 [23] kasutab kahte peamist standardit - platvormide ülest lahendust veebiautentimiseks WebAuthn [24] ning kliendi autentimisprotokolli CTAP (joonis 1). Kasutaja jaoks on selline autentimine lihtne ainulogimisega ligipääs (SSO). See tähendab seda, et kui seade on korra registreeritud, siis piisab seadmesse logimisest selleks, et pääseda ligi erinevatele autentimist nõudvatele andmetele ja rakendustele ilma rakenduse põhise autentimiseta.

Microsofti juhendi "How Windows Hello for Business works in Windows devices" [25] põhjal saab välja tuua, et Windows Hello seadistamiseks on vajalik kaheastmeline kinnitamine. Esimene samm sellest on seadme registreerimine. Selliseks seadme ning kasutajakonto autentimiseks ja sidumiseks on tavakasutajal kaks valikut - luua lokaalne konto või autentida identiteeditarnija Microsofti konto kaudu. Organisatsioonidel on identiteeditarnijaks Active Directory (AD) või Azure AD [26]. Microsofti konto ja lokaalse konto avaliku võtme loomisest, krüpteerimise andmest, selleks kasutatud moodultest ning andmete asukohast süsteemis on hea ülevaade E.Kim ja H-K.Choi uurimuses [27]. Kui identiteeditarnija on kasutaja autentinud või

lokaalne konto on loodud, lisab kasutaja teise sammuna PIN-koodi või žesti, milleks võib olla biomeetriline andmestik nagu sõrmejälg või näotuvastus.



Joonis 1. FIDO2 arhitektuurikompnentide ülevaade [58]

Windows Hello ja TPM

Et mõista täpsemalt Windows Hello teenust võetakse järgneva osa kirjelduse aluseks Microsofti dokumentatsiooni "Windows Hello for Business" [28,18].

Selleks, et turbeprotsessorit oleks võimalik eristada pahavarast, mis käitub nagu TPM, on vajalik järgmiste võtmete olemasolu:

a) Viseerimisvõti - selle võtme loob tootja seadme arendamisel otse turbeprotsessorisse. Võtme sertifikaat on signeeritud tootja poolt ja selle olemasolu näitab, et viseerimisvõti on turbeprotsessoris olemas. Sertifikaati saab kasutada koos viseerimisvõtit sisaldava turbeprotsessoriga selleks, et välistada erinevate stsenaariumite korral turbeprotsessoreid, mis käituvad nagu TPM aga tegelikult on pahavara. Ükski turbeprotsessori stsenaarium ei kasuta viseerimisvõtit otse.

b) Atesteerimisvõti - võti viseerimisvõtme tõestuseks. Viseerimisvõtmele on ligipääs identiteedi sertifikaadi autoriteedil (CA), kes kasutab viseerimisvõtit ja selle sertifikaati selleks, et tõestada ühe või rohkema atesteerimisvõtme reaalset olemasolu turbeprotsessoris. CA väljastab atesteerimisvõtme sertifikaate.

Windows Hello raamistikus on Microsoft identiteedi sertifikaadi autoriteet. Microsoft saab atesteerimisvõtme sertifikaate väljastada igale seadmele, kasutajale ja identiteeditarnijale. Sellega tagatakse, et turbeprotsessori nõuded on täidetud enne kui Windows Hello mandaadid eelmainitud üksustele kättesaadavaks tehakse.

Kui seadmel on TPM, siis genereerib see Windowsi Hello raamistiku kasutusele võtmisel asümmeetrilise võtmepaari ning kaitseb seejuures privaatset võtit. Kui seadmel turbeprotsessorit ei ole või see on välja lülitatud, siis privaatne võti krüpteeritakse ja see on kaitstud tarkvara poolt. Seega seadme registreerimisel seotakse avalik võti kasutajakontoga - hoiustatakse seda kas Microsofti serveris või lokaalselt. Teise sammuna luuakse võtmepaarile nii öelda turvavõti, mille kasutamisel on kasutajal õigus ligi pääseda esimeses sammus loodud Windows Hello mandaadile. Kui PIN lähtestatakse, siis luuakse alati uus asümmeetriline võtmepaar.

Windows Hello raamistikus on kaks kontseptsiooni:

a) Windows Hello for Business (WHfB), mille korral kasutaja läbib kaheastmelise kinnitamise. Selle käigus luuakse asümmeetriline võtmepaar, mis on turbeprotsessori poolt kaitstud. Organisatsioonidel võimaldab WHfB luua erinevaid poliitikaid, et hallata turvalist autentimist asutuse seadetes [29]. Konsepti nimes olev "*for Business*" on tavakasutajale segadust tekitav, sest turbeprotsessori olemasolul ja kaheastmelise kinnitamise korral, kasutab ka tavakasutaja seade siiski Windows Hello for Business kontseptsiooni. Seetõttu on töös edaspidi Windows Hello all mõeldud just seda. WHfB raamistiku autentimismeetodid on PIN ning biomeetriline autentimine.

b) Windows Hello mugavus PIN (Windows Hello convenience PIN) korral on tegemist seadmepõhise unikaalse autentimisega, mis kasutab tavalist sümmeetrilist parooliräsi. Võrreldes asümmeetrilise võtmepaariga, mis on turbeprotsessori poolt loodud ja kaitstud, on Windows Hello mugavus PIN tunduvalt ebaturvalisem. Seda konseptsiooni kasutatakse siis kui seadmel pole turbeprotsessorit või see on seadme registreerimise ja sisselogimissuvandite häälestamise ajal välja lülitatud. Autentimiseks on võimalik ka sellisel juhul kasutada PIN-koodi, biomeetrilist logimist ning lisaks tavapärast parooli ning piltparooli (*picture password*). Piltparooli puhul valib kasutaja autentimiseks pildi ning sellega koos kasutatavad puuteekraani liigutused. Puuteekraani liigutusi peab olema kolm ja need võivad olla ringid, sirgjooned või koputused. Seejuures on oluline nende ulatus, paigutus ning suund pildil.

Järgnevalt kirjeldatakse täpsemalt Windows Hello raamistiku sisselogimissuvandeid, milleks on turbeprotsessori funktsionaalsust kasutavad autentimised nagu biomeetriline ja PIN-koodiga autentimine.

PIN-koodiga autentimine

Lähtudes Microsofti artiklist "Why a PIN is better than a password" [30] on järgnevalt välja toodud PIN-koodiga autentimise ja parooli kasutamise erinevused.

Windows Hello raamistik adresseerib järgmisi probleeme:

1) tugevaid paroole on raske meelde jätta. Seetõttu kasutatakse paroole erinevates rakendustes ja seadetes korduvalt, mis teeb paroolid haavatavaks sõnastikrünnete jaoks;
2) serverimurde tulemusena võivad avalduda sümmeetrilised võrgumandaadid (paroolid);
3) paroolid on taasesitusrünnete sihtmärkideks;
4) kasutajad võivad andmepüügirünnakute käigus avaldada oma paroole.

Parool, Microsofti [30] süsteemide kontekstis, on sümmeetriline võti, mille räsi on salvestatud serverisse või lokaalsesse seadmesse. Seega on serverimurde ja taasesitus-, sõnastik- ning andmepüügirünnete korral parool haavatav.

Sellise parooli alternatiiviks on Windows Hello raamistikus PIN-kood, mis tuleb seadistada olenemata seadme biomeetrilise autentimise võimekusest. Näiliselt on PIN sama mis parool, sest seda saab määrata keerukaks ja pikaks sümbolite jadaks. Sisuliselt aga on nad erinevad. Seadistamisel seotakse PIN spetsiifilise seadmega, seega iga uue seadme kasutusele võtmiseks

on vaja luua uus PIN-kood. Mis on aga kõige olulisem - nagu ka eespool kirjeldatud, luuakse asümmeetriline võtmepaar, mis on kaitstud seadme turbeprotsessori poolt.

Biomeetriline autentimine

Võttes aluseks Microsofti artikli "Windows Hello for Business Overview" [22] on järgnevalt kirjeldatud Windows Hello biomeetrilise autentimise tehnoloogiat. Windows Hello pakub turvalist ja täielikult integreeritud biomeetrilist autentimist. Seejuures toetab see kaht biomeetrial põhinevat autentimist:

1) Näotuvastus kasutab spetsiaalseid kaameraid, mis näevad infrapunavalgust (infrapunakaamerad). See võimaldab tuvastada erinevused pildi, skaneeritud pildi ja reaalse inimese vahel. Paljud sülearvuti tootjad on infrapunakaamerad lisanud kallima klassi seadmete põhivarustusse ning mitmed tootjad pakuvad väliseid infrapunakaameraid, mis ühilduvad Windows Hello autentimistehnoloogiaga.
2) Sõrmejälje tuvastus kasutab mahtuvuslikku sõrmejälje sensorit. Sõrmejälje tuvastus on Windowsi arvutites juba aastaid, kuid praegune generatsioon sensoreid on tunduvalt turvalisemad ja vähem vea-altimad sarnanedes nutitelefonides kasutatavatele sensoritele.

Selleks, et tagada parim töökindlus ja kaitse kontrollib Microsoft [31] biomeetrilises autentimises kasutatavatele seadmete ja sensoritele seatud nõudeid (tabel 1), mis põhinevad kahel teguril. Üks neist on väärjaatustegur (FAR), mille korral biomeetrilise autentimise lahendus kinnitab volitamata isikut. Teine on vääreitustegur (FRR), mille korral biomeetrilise autentimise lahendusel ebaõnnestub volitatud isiku tuvastamine. Lisaks on mõlemal biomeetrial põhineval autentimisel nõutud teesklustõrje.

Tabel 1. Microsofti poolt aktsepteeritav väärjaatusteguri ning vääreitusteguri jõudlusvahemik sõrmejälje ning näotuvastuse sensoritele [32]

Sensori tüüp	FAR	FRR
Sõrmejälje puutesensorid	<0.001 – 0.002%	<10%
Sõrmejälje libistussensorid	<0.002%	<10%
Näotuvastuse sensorid	<0.001%	<10% (ilma teesklustõrjeta <5%)

Microsofti materjali [31] põhjal saab väita, et Windows Hello poolt kasutatud biomeetrilised andmed hoiustatakse turvaliselt ainult lokaalses seadmes. Biomeetrilisi andmeid ei saadeta kunagi välistele seadmetele ega serveritesse. Seetõttu ei saa ründaja andmeid varastada ja kui ründajal siiski leidub võimalus seadmest biomeetrilised andmed kätte saada, ei ole neid võimalik töödelda biomeetrilise sensori poolt tuvastatavaks mustriks. Iga seadme sensor omab biomeetrilise andmebaasi faili, kuhu andmemallid salvestatakse. Igal andmebaasil on unikaalne

juhuslikult genereeritud võti, mis on süsteemi krüpteeritud. Sensorite andmemallid krüpteeritakse andmebaasi põhise võtmega kasutades progressiivset krüpteerimisstandardit (AES) koos CBC-tööviisiga, mille räsi on SHA256. Mõned sõrmejäljelugejad hoiavad neid andmeid aga sensori enda moodulis, mitte operatsioonisüsteemis.

Lisaks biomeetrilisele ja PIN-koodiga autentimisele on võimalik end autentida eraldiseisva turvavõtmega, milleks võib olla USB-seade, kiipkaart või ka NFC seade. Neid saavad organisatsioonid ja tavakasutajad endale osta erinevatelt edasimüüjatelt (näiteks Yubico, Titan) [33].

1.3 BitLocker

Järgnev BitLockeri tehnoloogia ning alapeatükkides kirjeldatud selgitus põhineb Microsofti materjalidel "Overview of BitLocker Device Encryption in Windows" [21] ja "How Windows uses the Trusted Platform Module" [18].

BitLockeri ketta krüpteerimine on Windowsi operatsioonisüsteemiga integreeritud andmekaitse funktsioon. Selle eesmärk on kaitsta andmeid varastamise või ebaseadusliku kõrvaldamise eest seadmest. BitLocker töötab nii turbeprotsessoriga kui ka ilma.

BitLocker koos turbeprotsessoriga võimaldab süsteemi tervikluse kontrolli enne seadme alglaadimist. Lisaks lukustab BitLocker koos turbeprotsessoriga tavapärase käivitusprotsessi kuniks kasutaja identifitseerib end PIN-koodiga. Kui BitLockerit kasutatakse ilma turbeprotsessorita, siis kasutajalt nõutakse seadme käivitamisel, talveunest äratamisel turvavõtit või parooli.

Kõige tavapärasem BitLockeri konfiguratsioon tükeldab kõvaketta mitmeks jaotiseks. Ühes jaotises on konfidentsiaalne info - operatsioonisüsteem ja kasutaja andmed. Teistes jaotistes hoitakse avalikku infot nagu alglaadimise komponente, süsteemi informatsiooni ja taastamise tööriistu. Teisi jaotisi kasutatakse niivõrd harva, et need ei pea kasutajale nähtavad olema. Kui jaotis, mis sisaldab operatsioonisüsteemi ja kasutaja andmeid ei ole krüpteeritud ning lisakaitseid pole, siis on võimalik installida lisaks teine operatsioonisüsteem ja selle kaudu esialgse operatsioonisüsteemi failiõigused üle kirjutada. Kui BitLocker on kasutusel ja midagi alglaadimises muutub, siis nii operatsioonisüsteemi kui ka kasutaja andmestikku jaotisele ei ole võimalik ligi pääseda. Seega kui kõvaketas või arvuti varastatakse, siis välja lülitatud seadme korral jäävad andmed jaotisel konfidentsiaalseks ja sisse lülitatud seadmetel on andmetele ligi pääsemiseks vajalik sisselogimine.

BitLockeri kasutajamugavus

Operatsioonisüsteemides Windows 10 ja Windows 11 on varasemate versioonidega võrreldes parandatud nii turvalisust kui ka kasutajamugavust. See tähendab, et kui seade vastab standardsetele riistvaraturbe nõuetele, on BitLockeri ketta krüpteerimine sisse lülitatud automaatselt: puhta installi korral, kui arvuti on esmakordseks kasutamiseks valmis seatud, initsialiseeritakse BitLocker operatsioonisüsteemi ja andmete jaotisesse puhta võtmega. Sellisel juhul kuvatakse File Exploreris kettal hoiatusikoon (pilt 1 vasakul). Hoiatusikoon eemaldatakse kui turbeprotsessori kaitse on loodud ja taastevõti on varundatud (pilt 1 paremal).

Pilt 1. Vasakul Bitlockeri poolt dekrüpteerimata ketas hoiatusikooniga ja paremal Bitlocker poolt krüpteeritud ketas ilma hoiatusikoonita

Üks variant selleks on logida sisse Microsofti kontoga, puhas võti eemaldatakse ning taastevõti laetakse Microsofti kasutajakontole. Sellega on turbeprotsessori kaitse loodud. Kui seade sellisel juhul nõuab taastevõtit, suunatakse kasutaja taastevõtme ligipääsu lingile ning sealt võtme saamiseks, peab kasutaja kontole sisse logima. Lisaks on taastevõtit võimalik varundada salvestades see faili või printides välja.

Kõige turvalisem on seadet krüpteerida nii, et iga bitt on kettal krüpteeritud, sealhulgas ka need osad, kus andmeid pole. See on kindlasti vajalik juhtudel, kus kettal on varasemalt olnud konfidentsiaalseid andmeid ja need on eemaldatud. Kui kasutajal on aga täiesti uus ketas, siis kogu ketta krüpteerimine ei ole mõttekas. Selleks, et krüpteerimise aega drastiliselt vähendada võimaldab BitLocker krüpteerida olemasolevaid andmeid. Uued andmed krüpteeritakse, kui need kettale salvestatakse. Olenevalt andmehulgast vähendab selline meetod krüpteerimise aega kuni 99% [21].

Varasemas BitLockeri versioonis oli kasutajal vajalik kõigepealt kettale ligi pääsemiseks võti sisestada ning seejärel end autentida. TPM kaitse võimaldab aga BitLockerile ainulogimisega ligipääsu (SSO). Seda on täpsemalt kirjeldatud järgmises BitLockeri turvalisusega seotud alapeatükis.

BitLockeri turvalisus

BitLockeri seadme krüpteerimine kasutab XTS-AES krüpteerimisalgoritmi. See kaitseb sellise krüpteerimise rünnakute eest, mis põhinevad šifreeritud teksti manipuleerimisel, et põhjustada lihttekstis etteaimatavaid muutusi. BitLocker toetab nii 128-bitist kui ka 256-bitist XTS-AES võtit. Varasemad BitLockeri versioonid kasutasid AES-CBC 128- ja 256-bitist algoritmi.

BitLocker toetub süsteemi tervikluse kontrollimisel turbeprotsessorile - BitLockeri seadistamisel luuakse turbeprotsessoris võti, mille kasutamist lubatakse aga ainult siis, kui alglaadimine toimub nii nagu oodatud. TPM ja süsteemi põhivara teevad koostööd, et kontrollida, kuidas süsteem käivitati. Tarkvara saadab turbeprotsessorile sisendi, mis kontrollib tarkvara või seadistuse näitajaid, mida on võimalik arvutada kasutades räsialgoritmi. Algoritm teisendab suure andmestiku väikeseks, statistikaliselt unikaalseks räsiväärtuseks. Süsteemi põhivaral on tuumik usalduskomponent (CRTM), mis krüpteerib tarkvara komponendi ja salvestab selle näitaja turbeprotsessorisse. Süsteemi põhivara ja operatsioonisüsteemi laadurid jätkavad protsessi, kontrollides enne käivitamist igat järgnevat tarkvaralist komponenti. Kuna enne iga komponendi käivitamist, saadetakse selle näitajad turbeprotsessorisse, ei saa komponent oma näitajaid ise kustutada. Seega igal alglaadimisprotsessi sammul on turbeprotsessorile edastatud käivitatava tarkvara ja seadistuste näitajad. Mingil hetkel käivitusprotsessis näitajate edastamine turbeprotsessorisse peatub. Turbeprotsessor annab operatsioonisüsteemi jaotise dekrüpteerimiseks võtme kasutada ainult siis, kui turbeprotsessori oodatud tulemused vastavad Windowsi

alglaadimishalduris arvutatud tulemustele. Kui näitajate väärtustes ootamatult muutub midagi ja operatsioonisüsteemi jaotisele ei ole võimalik ligi pääseda, võimaldab BitLocker kasutada taastevõtit. Selle seadistamise võimalused on kirjeldatud eespool BitLockeri kasutajamugavuse alapeatükis.

Selline käivitusprotsess toimub taustal. Kui see on peatunud ning seadmel on seadistatud Windows Hello, lukustab BitLocker koos turbeprotsessoriga edasise käivitusprotsessi kuniks kasutaja identifitseerib end. Seega võimaldab TPM kettale ainulogimisega ligipääsu. Võrdluseks, kui BitLockerit kasutatakse ilma turbeprotsessorita, siis kasutajalt nõutakse seadme käivitamisel turvavõtit või parooli.

2 UEFI Turvaline käivitus

Teine oluline nõue operatsioonisüsteemis Windows 11 on, et seadme põhivara peab toetama UEFI turvalist käivitust. R. Wilkins ja B. Richardson toovad oma artiklis [10] välja, et operatsioonisüsteemide ja antiviiruse tarkvara tarnijad on karmistanud oma koodi ning sellest tulenevalt on pahavara arendajad võtnud sihiks rünnata alglaadimise eelset keskkonda. Kõige levinumad sellised rünnakud on juurkratid(*rootkit*) ja buutkratid(*bootkit*). Selleks, et süsteemid selliste rünnete eest oleksid vähem haavatavad loodi UEFI Foorumi poolt UEFI turvaline käivitus. Microsofti sellekohasele materjalile [34] toetudes on turvaline käivitus standard, mille eesmärk on tagada, et seade laeb käivitades ainult usaldusväärset tarkvara. Turbeprotsessor üksi seda eesmärki ei täida, sest TPM suudab küll alglaadimist kontrollida, kuid selliselt käivitatakse süsteem olenemata, kas seal on pahavara või ei. Turvaline käivitus aga tagab, et järgmine samm alglaadimises ei ole tehtud enne kui eelnev samm on hinnatud ohutuks. Turvaline käivitus ei ole turbeprotsessori olemasolust sõltuv ja on eraldiseisev turbetehnoloogia, mille täpsemad riistvaralised nõuded on leitavad Microsofti dokumentatsioonist[8]

Võttes aluseks nii Wilkins ja Richardsoni artikli [10] kui ka Microsofti turvalise käivituse dokumentatsiooni [34], on ilma muutusteta alglaadimise tagamiseks vaja kasutada digitaalset signatuuri. Digitaalne signatuur on sisse kirjutatud igasse koodi jaotisesse, mida on võimalik käivitada. Koodi looja allkirjastab koodi kasutades selleks privaatvõtit. Enne koodi käivitamist, kontrollitakse avaliku ja privaatvõtme abil, kas signatuur on dekrüpteeritav. Seega kui seade käivitub, kontrollib püsivara selliselt iga alglaadimisel käivitatava tarkvara signatuuri. Sealhulgas kontrollitakse ka UEFI põhivara draivereid, rakendusi ning operatsioonisüsteemi ennast. Kontrolli annab põhivara üle operatsioonisüsteemile vaid siis, kui signatuurid on kehtivad.

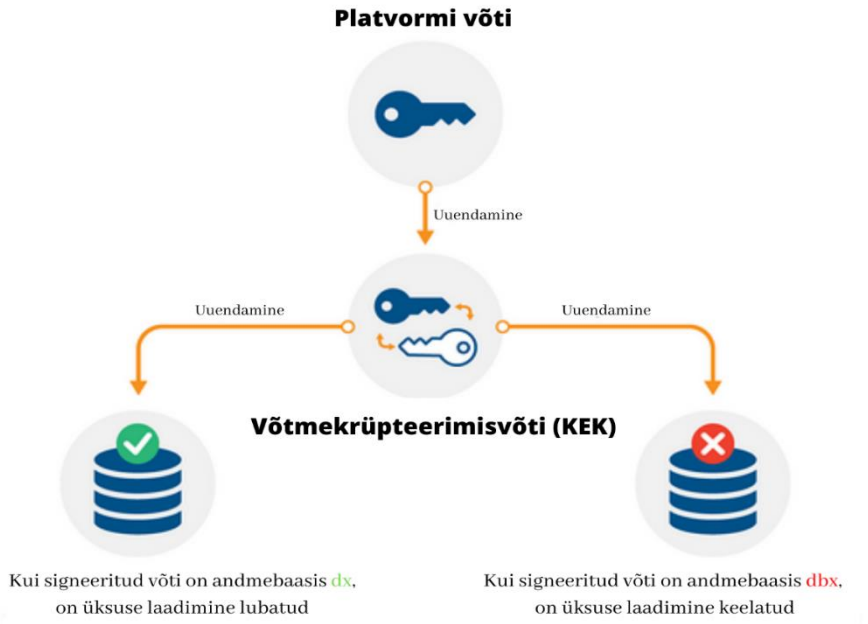
2.1 Signatuurandmebaasid ja võtmed

Et paremini aru saada turvalise käivituse andmebaasidest (joonis 2), võetakse järgneva peatüki kirjeldamise aluseks Microsofti dokumentatsioon “Secure Boot” [34].

Turvalise käivituse andmebaasid laetakse põhivara säilmällu tootmise ajal. Need sisaldavad signatuurandmebaase, tühistatud signatuuride andmebaase ja võtmekrüpteerimisvõtme andmebaase (KEK).

Signatuurandmebaasid ja tühistatud signatuuride andmebaasid sisaldavad UEFI rakenduste ja operatsioonisüsteemi laadijate (Microsoft OS laadija või alglaadimishaldur) signeerijat või räsi. Lisaks ka UEFI draivereid, mida saab seadmele laadida. Tühistatud signatuuride andmebaasid sisaldavad üksusi, mida enam ei usaldata ja mida ei saa laadida. Kui räsi on mõlemas andmebaasis, siis võetakse aluseks tühistatud signatuurandmebaas. KEK andmebaas on eraldi andmebaas signeeritud võtmetega, mida kasutatakse selleks, et värskendada signatuur- ja tühistatud signatuuride andmebaase. Microsoft nõuab spetsiaalse võtme olemasolu KEK andmebaasis, selleks, et tulevikus lisada uue operatsioonisüsteemi räsi signatuurandmebaasi ning vajadusel lisada ka teadaolevad halvad räsid tühistatud signatuuride andmebaasi.

Kui need andmebaasid on lisatud, valideeritud ning testitud, lukustab OEM põhivara, selliselt, et andmebaaside struktuure enam muuta ei saa. Andmete värskendamine ja muutmine on võimalikud vaid omades selleks signeeritud korrektset võtit. Teine variant andmebaaside muutmiseks on füüsiliselt seadmele ligipääseval kasutajal, kes kasutab selleks põhivara menüüsid ja genereerib platvormi võtme (PK). Platvormi võtmega saab signeerida uuendusi ning turvalist käivitust välja lülitada (joonis 2).



Joonis 2. Turvalise käivituse signatuurandmebaasid ja võtmed [35]

Kokkuvõtvalt Microsofti materjali [34] põhjal on sündmuste jada seadme käivitamisel turvalise käivituse korral järgmine (lisa 1):

1) Kui seade on sisse lülitatud, kontrollitakse signatuurandmebaase vastu platvormi võtit.
2) Juhul kui põhivara ei ole usaldusväärne, alustab UEFI põhivara OEMi põhise turvalise põhivara taastamise.
3) Juhul kui tekib probleeme Windowsi alglaadimishalduriga, laeb põhivara alglaadimishalduri varukoopia. Kui see ebaõnnestub, laeb põhivara OEMi põhise parandusmeetme.
4) Kui alglaadimishaldur töötab ja tekib probleem draiveritega või hübriidtuumaga, siis laetakse Windowsi taastamise keskkond. Selle abil taastatakse draiverid ja tuuma pilt.
5) Windows laeb viirusetõrje tarkvara.
6) Windows laeb ülejäänud tuuma draiverid ja alustab kasutaja režiimi.

Kuigi UEFI Turvaline käivitus üksi ei eemalda kõiki turvariske, on oluline, et operatsioonisüsteemi käivitamise eelne aeg oleks kontrollitud. Turvaline käivitus koos püsivara turvalise värskendamise tehnikate ja kontrollitud alglaadimisega, vähendab pahavara ründeid enne kui pahavaratõrje tarkvara käivitub.

[8] https://docs.microsoft.com/et-ee/windows-hardware/design/device-experiences/oem-secure-boot

3 Virtualiseerimispõhine turvalisus

Windows 11 operatsioonisüsteemile on Microsoft seadnud [36] ka kolmanda riistvaralise nõude ja seda protsessorile. See tuleb otsesest seosest virtualiseerimispõhise turvalisuse (VBS) tehnoloogiast. Nõue on seatud seetõttu, et VBSi toetavad uuemad 64-bitised protsessorid, millel on virtualiseerimise liidesed ja mälu terviklust toetavad süsteemidraiverid. Vajalikud virtualiseerimise liidesed on Intel VT-X koos EPT lahendusega [37] ning AMD-v koos RVI lahendusega [38]. Windows 11 ühilduvad protsessorid [39]:

1) Intel 11-nda generatsiooni Core protsessorid ja uuemad;
2) AMD Zen 2 arhitektuuriga protsessorid ja uuemad;
3) Qualcomm Snapdragon 8180 ja uuemad.

3.1 Mälu terviklus

VBS kasutab riistvara virtualiseerimise funktsioone, et eraldada operatsioonisüsteem turvalisest osast mälust. See võimaldab kogu süsteemi kaitsta operatsioonisüsteemis esinevate turvaaukude vastu ning pakub lisakaitset rünnete eest, mis on tehtud operatsioonisüsteemi kaitse suunal. Üht sellist funktsiooni HVCI ehk mälu terviklust kirjeldab Microsoft oma dokumentatsioonis [36]. Sama materjali põhjal kasutab HVCI virtualiseerimispõhist turvalisust selleks, et tugevdada koodi tervikluse poliitika jõustamist. Tuumarežiimi koodi tervikluse kontroll vaatab üle kõik draiverid ja binaarfailid enne nende käivitamist, takistades signeerimata draiverite või süsteemifailide laadimist süsteemimällu. Mälu terviklus loob virtuaalselt turvalise režiimi, kus piiratakse õigusi selleks, et kaitsta süsteemi töötamiseks vajalikke osi, operatsioonisüsteemi ressursse ning turvavarasid nagu seda on kasutaja mandaadid. Kasutajarežiimis muudetav koodi tervikluse poliitika kontrollib rakendusi enne kui need käivitatakse ja käivitab ainult need, mis on signeeritud teada tuntud signeerijate poolt. Kuna mälu tervikluse funktsioon töötab turvalises keskkonnas, kaitseb see kerneli viiruste ja pahavara vastu. Hüperviisor, mis on kõige kõrgemate õigustega süsteemitarkvara, määrab lehekülgede õiguseid üle kogu süsteemi. Leheküljed tehakse käivitatavaks alles siis, kui mälu tervikluse kontrollid on turvalises osas läbitud. Käivitatavad lehekülgi ei saa üle kirjutada ega muuta ja muudetud mälu ei saa käivitatavaks muuta.

Mälu terviklus on kasutajaliidese poolelt lihtsasti sisse ja väljalülitatav. Selle kohta on täpsemalt selgitatud töö praktilises osas peatükis 7.1.

3.2 Protsessori mudelipõhiste registrite kaitse

Kui mälu tervikluse üle on kasutajal operatsioonisüsteemi rakenduse kaudu kontroll, siis virtualiseerimispõhise turvalisusega kaasneb ka taustal töötavaid erinevaid funktsioone. Üks selline kaitse on otseselt protsessoriga seotud mudelipõhiste registrite kaitse.

Võttes aluseks Windowsi virtualiseerimispõhise turvalisusega seotud materjali [40] eeldab hüperviisor, et pahatahtlik kood võib Windowsi tuuma kahjustada. Seega peab hüperviisor kaitsma olulisi süsteemiressursse tuumarežiimis töötava pahatahtliku koodi eest. Ühed sellised olulised süsteemiressursid on protsessori mudelipõhised registrid. Kaasaegsed protsessorid

toetavad paljusid mudelipõhiseid registreid, millest suurem osa kontrollivad protsessori käitumist. Registritele pääseb ligi indekside kaudu, mis on unikaalsed mudelipõhiste registrite identifikaatorid. Ajalooliselt on mudelipõhised registrid arhitektuurilised, mis tähendab, et nad on mitme protsessori generatsiooni üleselt samad ja muutumatud. Sellised dokumenteeritud ja indekseeritud mudelipõhised registrid on usaldusväärsed teada ja avalikustatud võimalustega. Just need mudelipõhised registrid, mis erinevad protsessorite lõikes ja mida on aja jooksul muudetud, on problemaatilised süsteemitaseme tarkvarale. Seega muutes mudelipõhiste registrite poolt kontrollitud seadeid, võimaldab pahatahtlik tuumarežiimi kood muuta süsteemi käitumist nii, et ründaja saab kontrolli süsteemi üle. Lisaks paljud mudelipõhised registrid sisaldavad infot süsteemi töötamise kohta. Seega peab hüperviisor tuvastama ja kaitsma mudelipõhiste registrite ebaõiget kasutust. Sellest tulenevalt jälgib ja kontrollib hüperviisor kõikide mudelipõhiste registrite ligipääsu. Hüperviisor omab mudelipõhiste registrite indeksite loendit ning võimaldab tuumarežiimi koodi ligipääsu ainult neile registritele (või teatud registri bittidele), mis ei kujuta endast turvariski. Kui mudelipõhine register on tundmatu või on avalikustatud dokumentatsiooni põhjal turvariskiga, siis hüperviisor blokeerib või võimaldab sellele vaid osalise juurdepääsu.

Kui hüperviisor on mudelipõhisele registrile ligipääsu blokeerinud, logib see üksikasjad Windowsi süsteemi logisse (Event Viewer). Seda teeb hüperviisor aga ainult siis, kui virtualiseerimispõhine turvalisus on sisse lülitatud ning töötab. Selle kontrollimine praktikas on välja toodud peatükis 7.1.

4 HP Elitebook 840 G8

Töö praktilises osas kasutatakse kaasaegset äriklassi sülearvutit HP Elitebook 840 G8. Tartu Ülikooli arvutiteaduste instituut pakub antud sülearvutit tudengitele alates 2021 aastast õpingute ajaks ning seega on levinud igapäevane õppetöö tegemise vahend. Varasemalt arvutiteaduse instituudi poolt pakutud seadmete spetsifikatsioonid ning nende vastavust turbenõuetele on võimalik lugeda lisast (lisa 2). Järgnevalt on välja toodud eelnevalt töös kirjeldatud turbetehnoloogiatega seotud konkreetsed seadmepõhised lahendused võttes aluseks HP Elitebook 840 G8 spetsifikatsiooni [41].

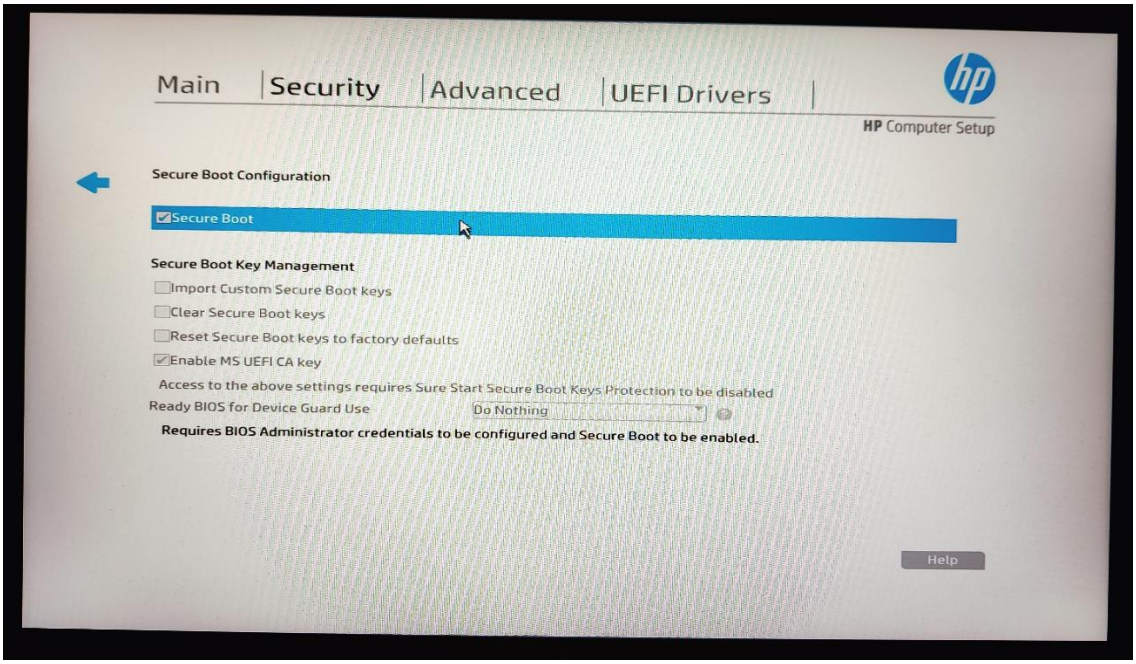
Seadmel on TPM 2.0 Infineon SLB9670, mis on süsteemiga integreeritud jada-välisliidese kaudu ja võimaldab edastuskiirust kuni 43 MHz (pilt 2). Täpsemalt saab erinevate sertifikaatide

Pilt 2. Turbeprotsessor 2.0 Infineon SLB9670 [60]

ja ülesehituse kohta lugeda seadme andmelehest [42]. Kuna antud TPM on versiooniga 2.0, vastab see Windows 11 nõuetele.

Teiseks oluliseks Windows 11 miinimumnõudeks on protsessori võimekus tagada virtualiseerimispõhine turvalisus koos mälu terviklusega. Elitebookil on selleks olemas protsessor i5-1135G7 baassagedusega 2.4GHz, Intel Turbo Boost tehnoloogiaga kuni 4.2 GHz. Seadme spetsifikatsiooni [43] järgi on sellel protsessoril VT-x koos EPT [37] tehnoloogiaga. Sellega on täidetud ka Windows 11 miinimumnõue protsessorile.

HP kasutajatoe [44] järgi on kõigil HP arvutitel, mis on toodetud Windows 10 jaoks, turvaline käivitus olemas ja UEFI püsivara liidesest vaikimisi sisse lülitatud (pilt 3). Seega on täidetud ka kolmas turbenõue Windows 11 jaoks.



Pilt 3. UEFI püsivara liideses turvaline käivitus (Secure Boot)

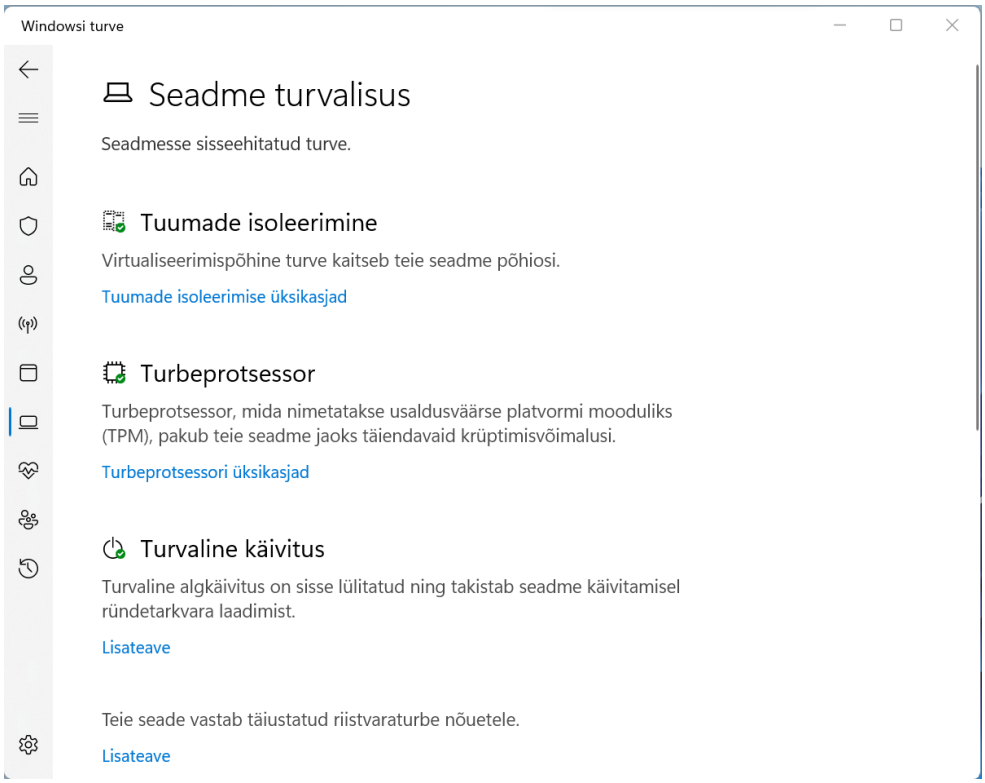
Seadmel on tavapärastele riistvaralistele lahendustele lisaks lähiväljaside ehk NFC, mis kasutab NXP Semiconductorsi toodetud HP moodulit koos NXP NFC kontroller NPC300 I2C NCI, sõrmejälje lugeja Synaptics FS7604 Touch Fingerprint Sensor koos PurePrint(™) ning kiipkaardi lugeja Microsoft Usbccid Smartcard Reader (WUDF). Seadmel on ka sisseehitatud HP infrapunakaamera, mille tootja on Quanta. Lisainfo antud seadme kohta on leitav Tartu Ülikooli arvutiteaduste instituudi seadmete tabelist lisas (lisa 2).

Seadme spetsifikatsiooni [41] järgi on HP Elitebook 840 G8 arendatud ennekõike operatsioonisüsteemile Windows 10. Seda toetab ka fakt, et Tartu Ülikooli poolt pakutaval seadmel on vaikimisi Windows 10 Pro litsents. Võttes aluseks aga eelnevalt välja toodud tehnoloogiad ja nende vastavus, siis ka Windows 11 on antud seadmele sobiv operatsioonisüsteem.

5 Turbetehnoloogiate praktiline kasutamine

Järgnevas peatükis on vaatluse all operatsioonisüsteemid Windows 10 Pro ja Windows 11 Pro ning eespool peatükkides läbi töötatud riistvaraturbe tehnoloogiate praktiline ülevaade HP Elitebook 840 G8 seadmel.

Mõlemad operatsioonisüsteemid võimaldavad kasutajal näha riistvaraga seotud turbetehnoloogiaid ja nende olekuid rakenduses Windowsi turve. Täpsemalt on kuvatud rakenduse alamenüüs "Seadme turvalisus" seadmesse sisseehitatud turbetehnoloogiate olekud. Turbelahendustena kuvatakse kõiki eespool lahti seletatud turbelahendusi - tuumade isoleerimine, turbeprotsessor ja turvaline käivitus (pilt 4).



Pilt 4. Rakendus Windowsi turve ning selle alamenüüs kuvatud turbetehnoloogiad

Kui turbeprotsessor ning turvaline käivitus on UEFI püsivara sätetest välja lülitatud, ei ole võimalik Windows 11 seadmele installida. Windows 10 operatsioonisüsteemi installeerides selline riistvaraline piirang puudub, kuid kontroll on siiski olemas (lisa 3). Kuna HP Elitebook 840 G8 on olemas nii turvaline käivitus kui ka turbeprotsessor ning vaikimisi on need ka tootja poolt sisse lülitatud, siis Windows 11 installimine toimub tõrgeteta. Kui kasutusel on aga seade, millel antud turbelahendused puuduvad, on Microsofti kasutajatugi välja toonud lahenduse operatsioonisüsteemi installimiseks[9]. See pole turvariski tõttu aga soovitatav kõrget turvalisust nõudvates süsteemides.

[9] https://support.microsoft.com/en-us/windows/ways-to-install-windows-11-e0edbbfb-cfc5-4011-868b-2ce77ac7c70e

Rakenduses Windowsi turve, kuvatakse tavakasutajale seadme turvalisuse astmega seotud teade [45]. Seal võib olla neli erinevat astet ja sellega seotud teadet:

1) Teade "Standardse riistvaraturbe toetus puudub" tähendab, et kasutajal on välja lülitatud vähemalt üks kolmest turbelahendusest - tuumade isoleerimine, turbeprotsessor või turvaline käivitus.
2) Teade "Teie seade vastab standardse riistvaraturbe nõuetele" tähendab, et kasutajal on sisse lülitatud kõik kolm turbelahendust.
3) Teade "Teie seade vastab täiustatud riistvaraturbe nõuetele" tähendab, et kasutajal on sisse lülitatud kõik kolm turbelahendust ning lisaks on sisse lülitatud ka mälu tervikluse funktsioon.
4) Teade "Teie seade ületab täiustatud riistvaraturbe nõuded" tähendab, et seadmel on sisse lülitatud kõik kolm turbelahendust, mälu terviklus ning lisaks ka süsteemihaldusrežiimi (SMM) kaitse.

Windows 11 puhta installi korral kuvatakse seadmel HP Elitebook kasutajale teade "Teie seade vastab täiustatud riistvaraturbe nõuetele". Windows 10 ja Windows 11 kui versioonitäiendi korral kuvatakse seal vaikimisi sättete korral "Teie seade vastab standardse riistvaraturbe nõuetele". Neljas turbeaste on mõeldud Windowsi Education ja Enterprise väljaannetele ning eeldab, et tuumade isoleerimise all on sisse lülitatud ka püsivarakaitse [46]. Kuna selle astme korral on tegemist väga kõrge turvatasemega, siis piiratud mahu tõttu ei ole antud töös püsivarakaitset ning süsteemihaldusrežiimi kaitsest kirjutatud.

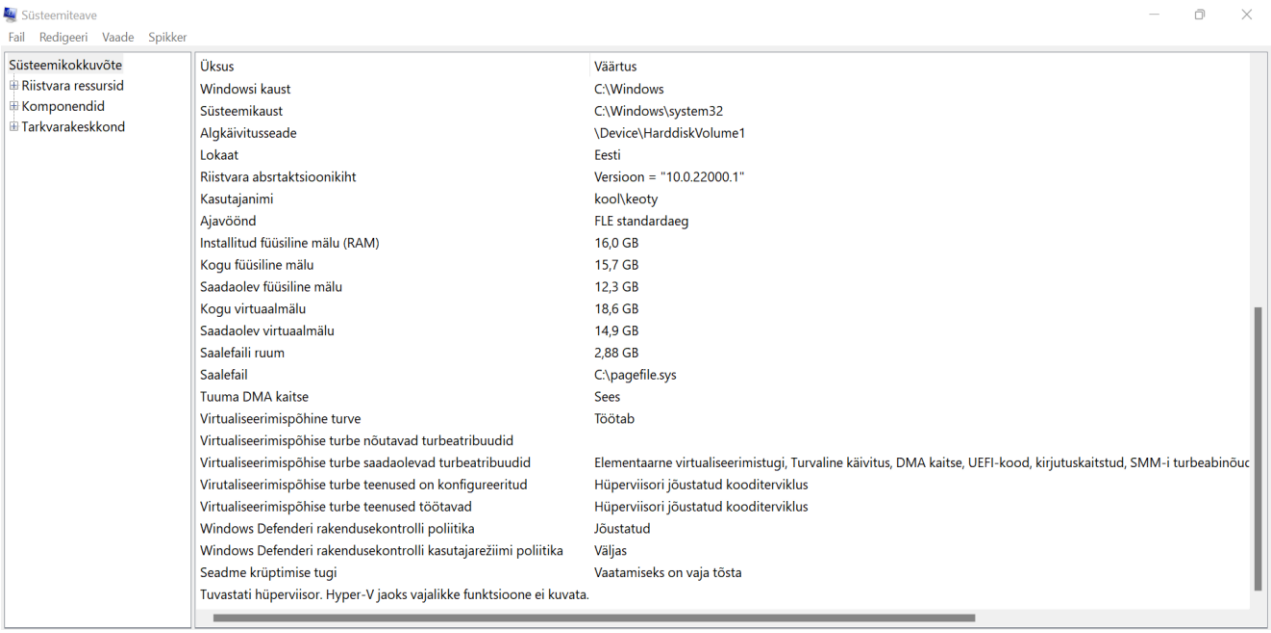
5.1 Virtualiseerimispõhine turvalisus

Virtualiseerimispõhine turvalisus, mis on Windowsi turbe rakenduses kui tuumade isoleerimine, sisaldab HP Elitebookil üksikasjade all mälu terviklust (HVCI) ja mällupöörduse kaitset (DMA kaitse) (tabel 2). Lisaks on Windows 10 ja Windows 11 Education ja Enterprise väljaannetel selles alammenüüs võimalus sisse lülitada ka püsivarakaitse [46].

Tabel 2. Tuumade isoleerimise turbelahenduste vaikeväärtused

Tuumade isoleerimise funktsioon	Windows 10	Windows 11 kui versioonitäiend	Windows 11 puhas install
Mälu terviklus	Välja lülitatud	Välja lülitatud	Sisse lülitatud
Mällupöörduse kaitse	Sisse lülitatud	Sisse lülitatud	Sisse lülitatud

Virtualiseerimispõhine turvalisus aga ei piirdu vaid sellega, mida kuvatakse kasutajale tuumade isoleerimise all. Virtualiseerimise info ja parameetrid on lisaks toodud ka rakenduses „Süsteemiteave“(pilt 5). Näiteks on peatükis 5.2 mainitud protsessori mudelipõhiste registrite kaitse sisse lülitatud kui antud rakenduses parameetri „Virtualiseerimispõhine turve“ väärtus on „Töötab“. Lisaks on näha seal ka teisi virtualiseerimispõhise turbega seotud teenuseid, mis enamasti töötavad taustal.



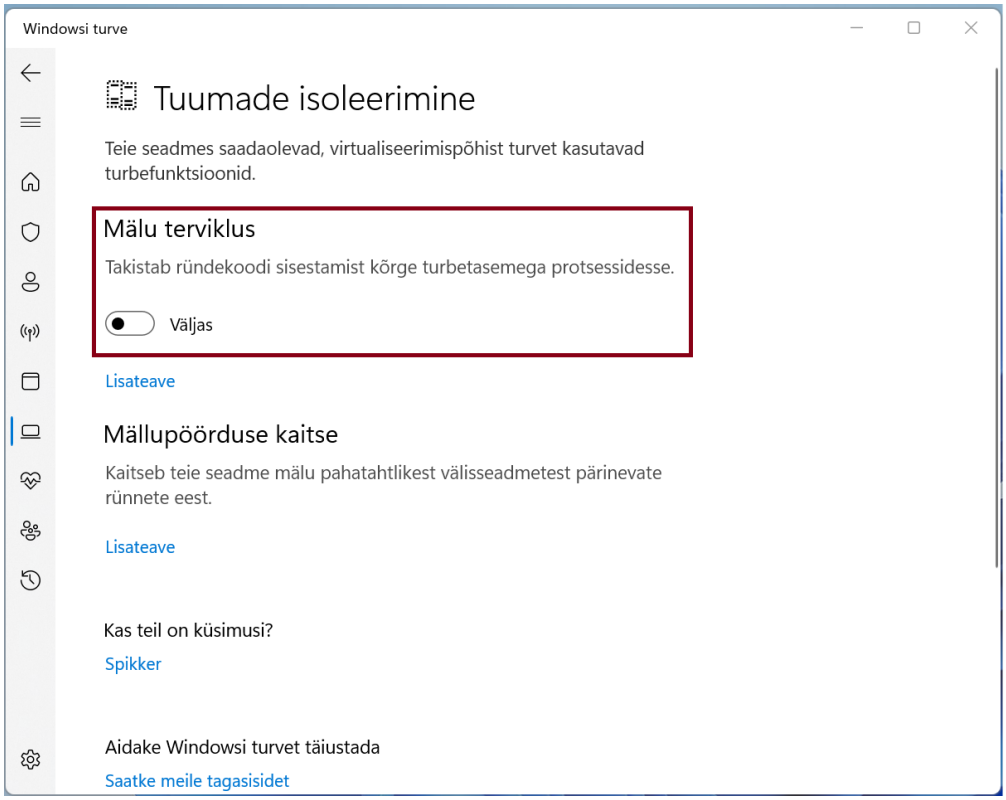
Pilt 5. Süsteemiteave

Mälu terviklus

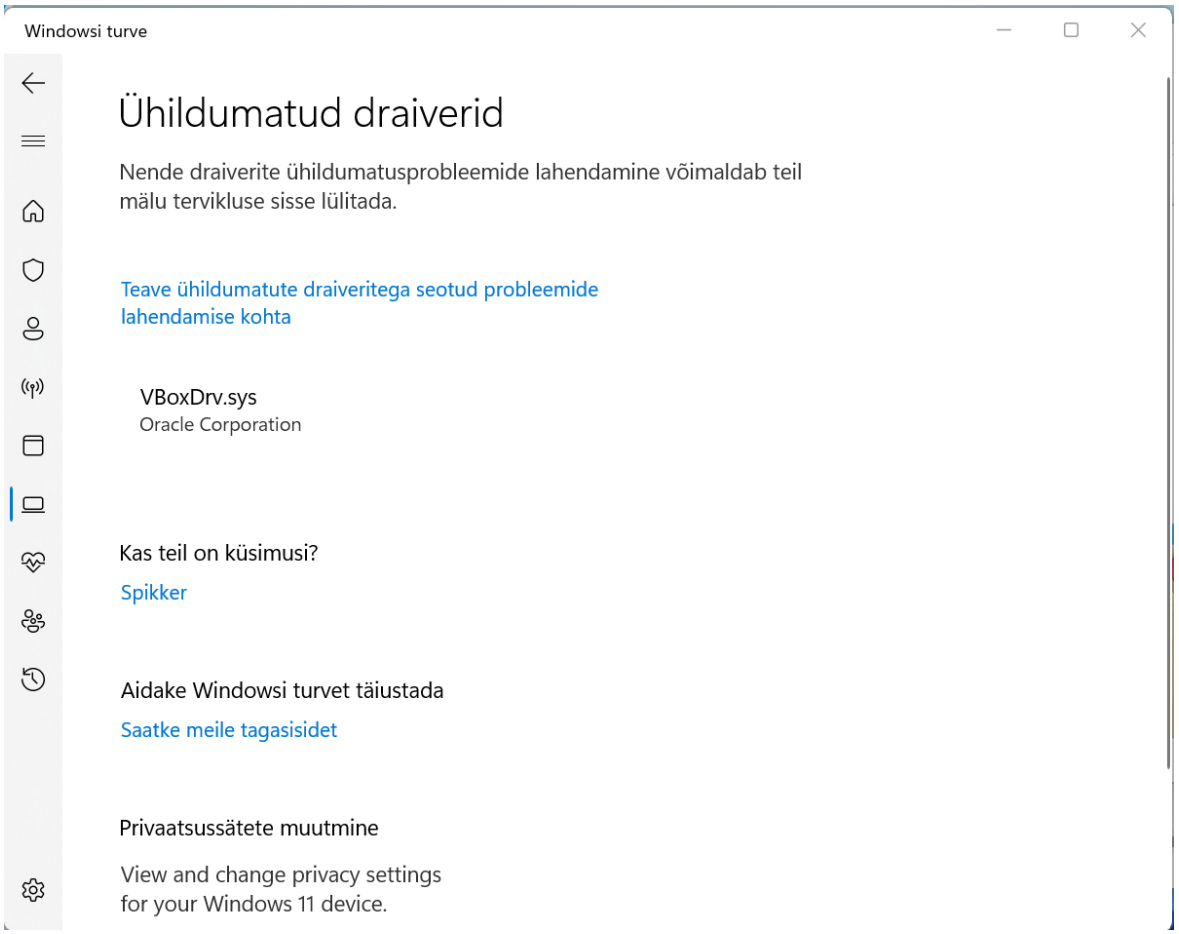
Microsofti dokumentatsioonis “Hypervisor-protected Code Integrity enablement” [47] tuuakse välja, et kui süsteem on mälu terviklusega ühilduv, siis puhta installi korral on alates Windows 11 operatsioonisüsteemist see vaikeväärtusena sisse lülitatud. Vaatluse all oleval seadmel leidis see fakt ka testimisjärgselt kinnitust. Nii Windows 10 kui ka Windows 11 (kui versioonitäiendi) installeerimisel on mälu terviklus vaikimisi aga välja lülitatud (tabel 2).

Mälu terviklus on Windowsi riistvaraturbe lahendustest ainus, mida saab Windowsi turve rakendusest kasutajaliidese kaudu lihtsasti ja mugavalt sisse ja välja lülitada (pilt 6). Mälu tervikluse sisse lülitamisega on tõenäosus, et süsteemis on selle turbelahendusega ühildamatuid draivereid. Sellisel juhul ei ole võimalik mälu terviklust kohe sisse lülitada ja kasutajale kuvatakse vastavasisuline teade (pilt 7). Kui mälu terviklus on sisse lülitatud ning kasutaja proovib seadmesse installida ühildamatut tarkvara, kuvatakse samuti kasutajale sellekohane teade (pilt 8). On oluline hinnata, kas vastav draiver on üldse süsteemis vajalik. Esimene samm on sellisel juhul kontrollida, kas tootja pakub draiveri ühildamiseks uuendust. Kui ei paku ja kasutaja sellegipoolest soovib mälu terviklust sisse lülitada, tuleb vastav draiver eemaldada.

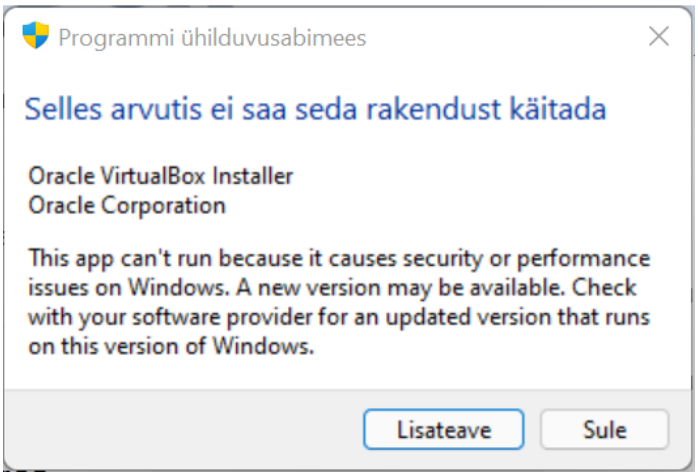
Puhta installi korral ei esine HP Elitebookil ühildamata draiveritega probleeme ning sellisel juhul on vaikimisi mälu terviklus sisse lülitatud. Juba kasutuses oleva HP Elitebooki puhul sõltub ühildamatute draiverite olemasolu seadmes kasutatavast tarkvarast. Levinud virtualiseerimist kasutavad tehnoloogiad, nagu Oracle Virtualbox ja VMware, ei ühildu virtualiseerimispõhiste turbelahendustega. See on Microsofti dokumentatsiooni [48] põhjal järeldades eeldatud käitumine. Siiski ka antud tarkvarade arendajad teevad pidevalt tööd, et parandada draiverite ühilduvust ja tehnoloogiate võimekust. Näiteks töö kirjutamise alguses Oracle Virtualbox 6.1.30 ei ühildunud mälu tervikluse gа (pilt 7-8), kuid 22.01.2022 tehtud versioonitäiendusega 6.1.32 oli tarkvara seadmesse paigaldamine võimalik.



Pilt 6. Mälu terviklus(HVCI) rakenduses Windowsi turve



Pilt 7. Windowsi turve vaade kui kasutaja soovib mälu terviklust sisse lülitada, kuid seadmes on mälu terviklusega ühildumatud draiverid.



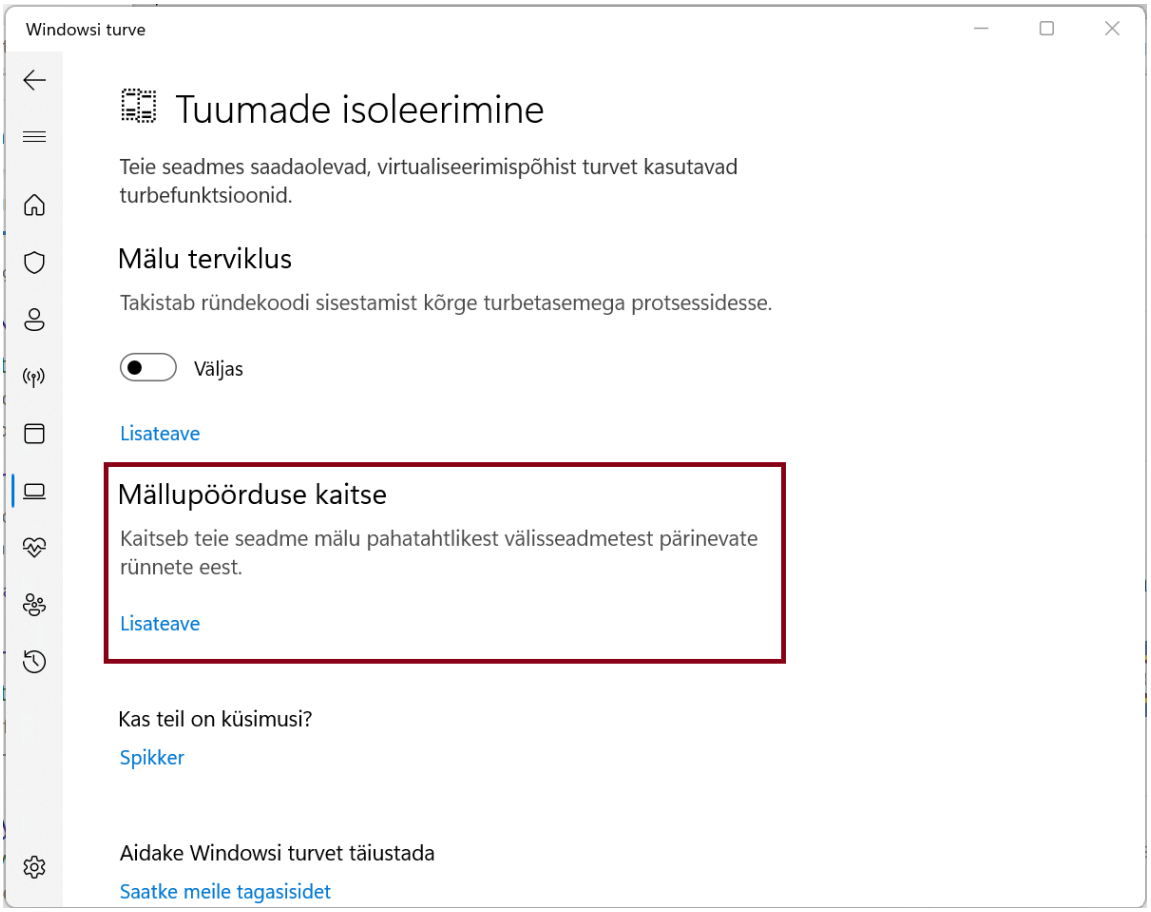
Pilt 8. Mälu terviklus on sisse lülitatud ja kasutaja soovib installeerida mälu terviklusega ühildumatut tarkvara.

Mällupöörduse kaitse

Mällupöörduse kaitse ehk tuuma DMA kaitse on tuumade isoleerimise alajaotuse all välja toodud, kuid Microsofti dokumentatsiooni [49] põhjal eeldades ei ole virtualiseerimine otseselt mällupöörduse kaitseks vajalik. Oma olemuselt on mällupöörduse kaitse eesmärk turvata

seadet otsemällupöörduse rünnakute vastu, mille sooritamiseks kasutatakse PCI seadmeid, mis ühendatakse väliselt PCIe portidesse. HP Elitebookil on selliseks pordiks Thunderbolt 4. Bakalaureusetöö piiratud mahu tõttu mällupöörduse kaitset töös väga põhjalikult ei kirjeldata, kuid soovi korral on võimalik sellest täpsemalt lugeda Microsofti dokumentatsioonist[10].

HP Elitebookil on mällupöörduse kaitse automaatselt sisse lülitatud mõlemas operatsioonisüsteemis (tabel 2). Kui see on sisse lülitatud, siis kuvatakse rakenduses vastavasisuline info (pilt 9). Kui tuumade isoleerimise üksikasjade all ei ole kuvatud vastavat infot, siis see tähendab, et see on välja lülitatud. Seda on see võimalik sisse lülitada UEFI püsivara sätetest (lisa 4). Siinkohal tasub tähele panna, et selle seadistuse väljalülitus teeb seadme DMA rünnetele haavatavaks ning kõrget turvalisust nõudvates süsteemides peaks see olema kindlasti sisse lülitatud operatsioonisüsteemides Windows 10 ja Windows 11.



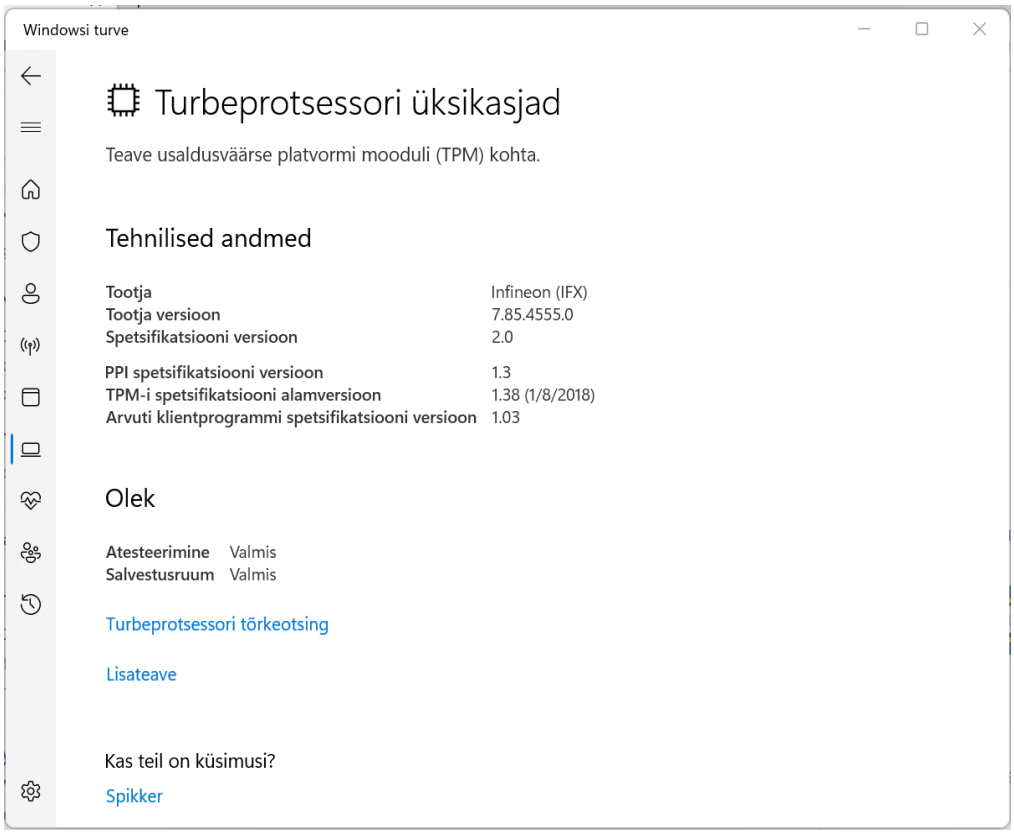
Pilt 9. Windowsi turve rakenduses tuumade isoleerimise alamenüüs mällupöörduse kaitse teade, mis tähendab, et mällupöörduse kaitse on aktiivne ja sisse lülitatud.

[10] https://docs.microsoft.com/en-us/windows/security/information-protection/kernel-dma-protection-for-thunderbolt

5.2 Turbeprotsessor

HP Elitebook 840 G8 seadmel on TPM mõlemas Windowsi versioonis vaikimisi kasutuses. Windowsi turbe rakendus võimaldab vaadata turbeprotsessori üksikasjade all teavet TPM tehniliste andmete ning oleku kohta (pilt 10).

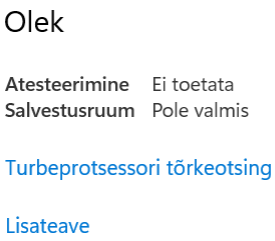
Tehniliste andmete all on info tootja ning tootja versiooni kohta. HP Elitebookil on tegemist Infineon (IFX) versiooniga 7.85.4555.0. Samuti on info turbeprotsessori spetsifikatsiooni üldise versiooni kohta, milleks on 2.0, millega määratakse TPM võimekus ning selle kohta saab täpsemalt lugeda peatükis 3. PPI (*Physical Presence Interface*) spetsifikatsiooni eesmärk on Trusted Computing Groupi veebilehe [50] põhjal tagada operatsioonisüsteemi ning BIOSi vaheline suhtlusmehhanism. HP Elitebookil on PPI spetsifikatsiooni versioon 1.3, mis on töö kirjutamise ajal kõige uuem PPI versioon. TPM-i spetsifikatsiooni alamversioon täpsustab TPM spetsifikatsiooni revisjoni numbrit – vaatluse all oleval seadmel on see 1.38. Arvuti klientprogrammi spetsifikatsioon on dokument, mis täiendab peamist TPM 2.0 spetsifikatsiooni platvormi spetsiifilise funktsionaalsusega. Täpsemat info spetsifikatsioonide kohta on leitav Trusted Computing Groupi veebilehelt[11,12,13].



Pilt 10. Turbeprotsessori olek rakenduses Windowsi turve.

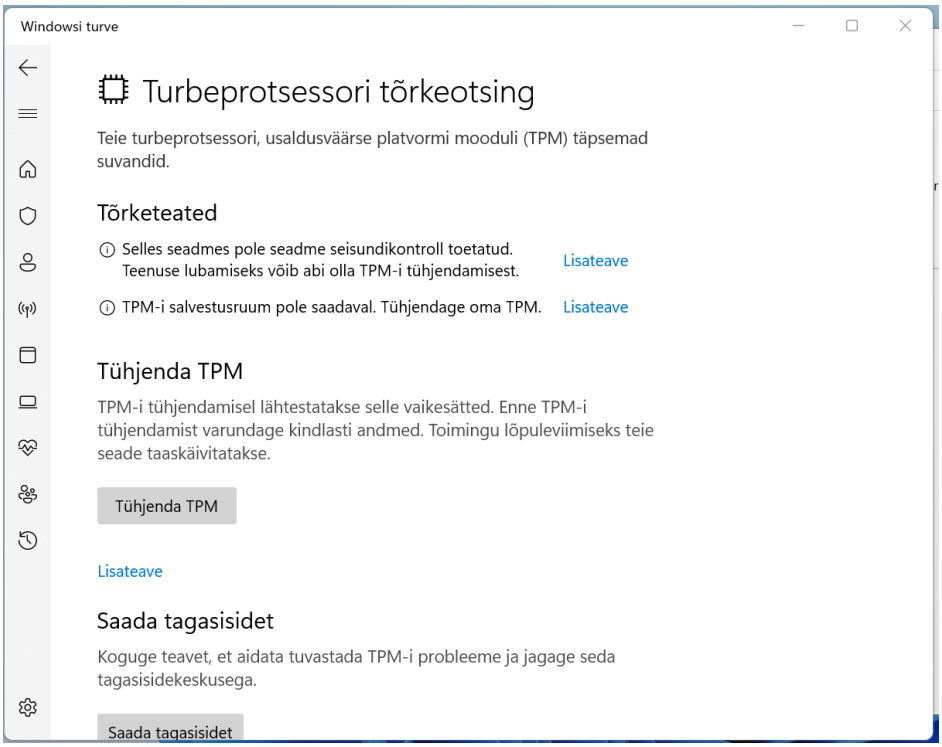
Lisaks on kuvatud turbeprotsessori atesteerimise ja salvestusruumi olek (pilt 10-11). Tehnilise dokumentatsiooni võtmete atesteerimisest leiab Microsofti materjalidest [51].

[11] https://trustedcomputinggroup.org/wp-content/uploads/Physical-Presence-Interface_1-30_0-52.pdf
[12] https://trustedcomputinggroup.org/resource/tpm-library-specification/
[13] https://trustedcomputinggroup.org/resource/pc-client-platform-tpm-profile-ptp-specification/

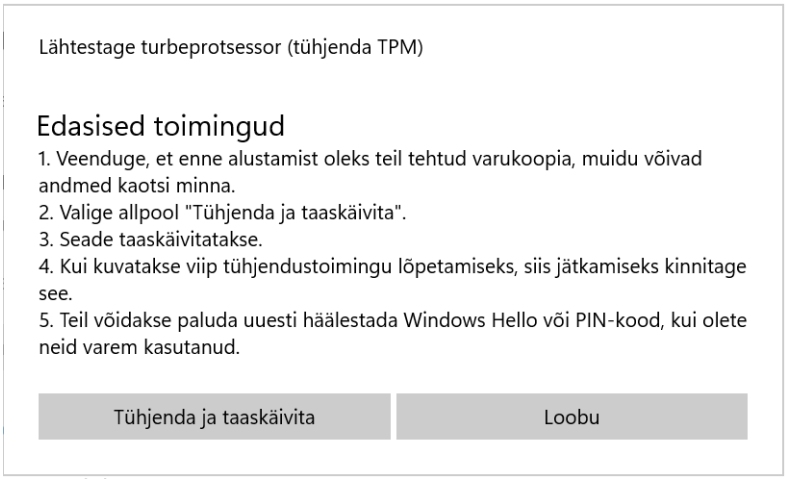


Pilt 11. Atesteerimise ja salvestusruumi olek kui TPM funktsionaalsus on välja lülitatud

HP Elitebookil on võimalik UEFI püsivaraliidest TPM välja lülitada nii, et turbeprotsessori olemasolu süsteemile on teada, kuid operatsioonisüsteem omaniku õiguseid kasutada ei saa (tabel 3). Sellisel juhul kuvatakse HP Elitebooki kasutajale Windows turbe rakenduses turbeprotsessori oleku all, et salvestusruum pole valmis ning atesteerimist ei toetata (pilt 11). Valides „Turbeprotsessori tõrkeotsing“ kuvatakse kasutajale avanevas aknas turbeprotsessori täpsemad suvandid: tõrketeated ning turbeprotsessori tühjendamise info (pilt 12). Osa võimalikke tõrketeateid on välja toodud Microsofti dokumentatsioonis [52]. HP Elitebooki turbeprotsessori tõrketeadetest lähtuvalt on iga tõrketeate juures antud võimalik lahendus ning lisateabe saamiseks ka link, mis suunab Microsofti kasutajatoe veebilehele. Enamikul juhtudest piisab turbeprotsessori tühjendamisest. Samas tuleb meeles pidada, et kõik turbeprotsessoriga kasutatud funktsionaalsused on muudatusest mõjutatud ning enamasti on vaja turbelahendused uuesti seadistada (nagu näiteks Windows Hello biomeetriline logimine). Vajutades „Tühjenda TPM“ nupul kuvatakse ka kasutajale vastavasisuline hoiatus (pilt 13).

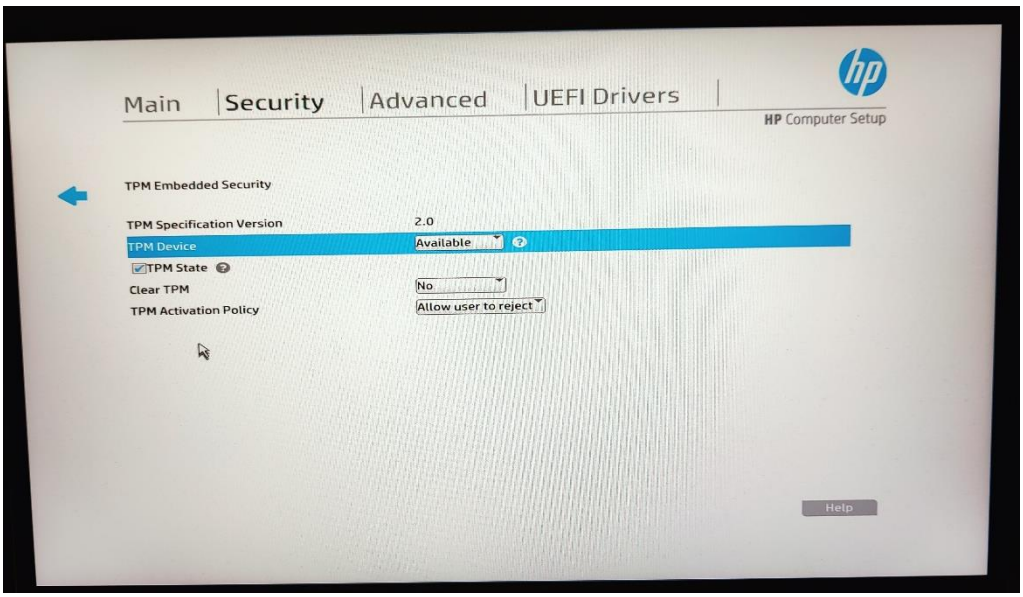


Pilt 12. HP Elitebook turbeprotsessori tõrkeotsingu vaade koos tõrketeadetega



Pilt 13. Turbeprotsessori tühjendamisel kuvatav lisainfo

Rakendusest ja operatsioonisüsteemi seadetest ei saa turbeprotsessorit välja lülitada. Selleks tuleb kasutada UEFI püsivara sätteid (pilt 14). HP võimaldab püsivara sätetest muuta TPM oleku erinevaid parameetreid (tabel 3). Selleks, et kogu seadmes olevad turbelahendused saaksid kasutada turbeprotsessori poolt pakutavaid krüpteerimisalgoritme ning võtmete salvestusruumi, ei ole turbeprotsessorit soovitav välja lülitada. Turbeprotsessori välja lülitamise vajadus tekib siis kui kasutajal on vaja ajutiselt installeerida teine operatsioonisüsteem paralleelselt olemasolevaga, samal ajal andmeid turvaliselt eraldades ja neile ligipääsu mitte andes. Lisaks on oluline, et kõrge turbetasemega seadmetes oleks parameeter TPM Activation Policy väärtuseks *Allow user to reject*, sest sellisel juhul on seadmes muudatuste kinnitamiseks vajalik kasutaja füüsiline kohalolek.



Pilt 14. HP Elitebook 840 G8 turbeprotsessori parameetrid UEFI püsivaraliides

Tabel 3.HP Elitebook 840 G8 UEFI püsivaraliideses turbeprotsessori parameetrid

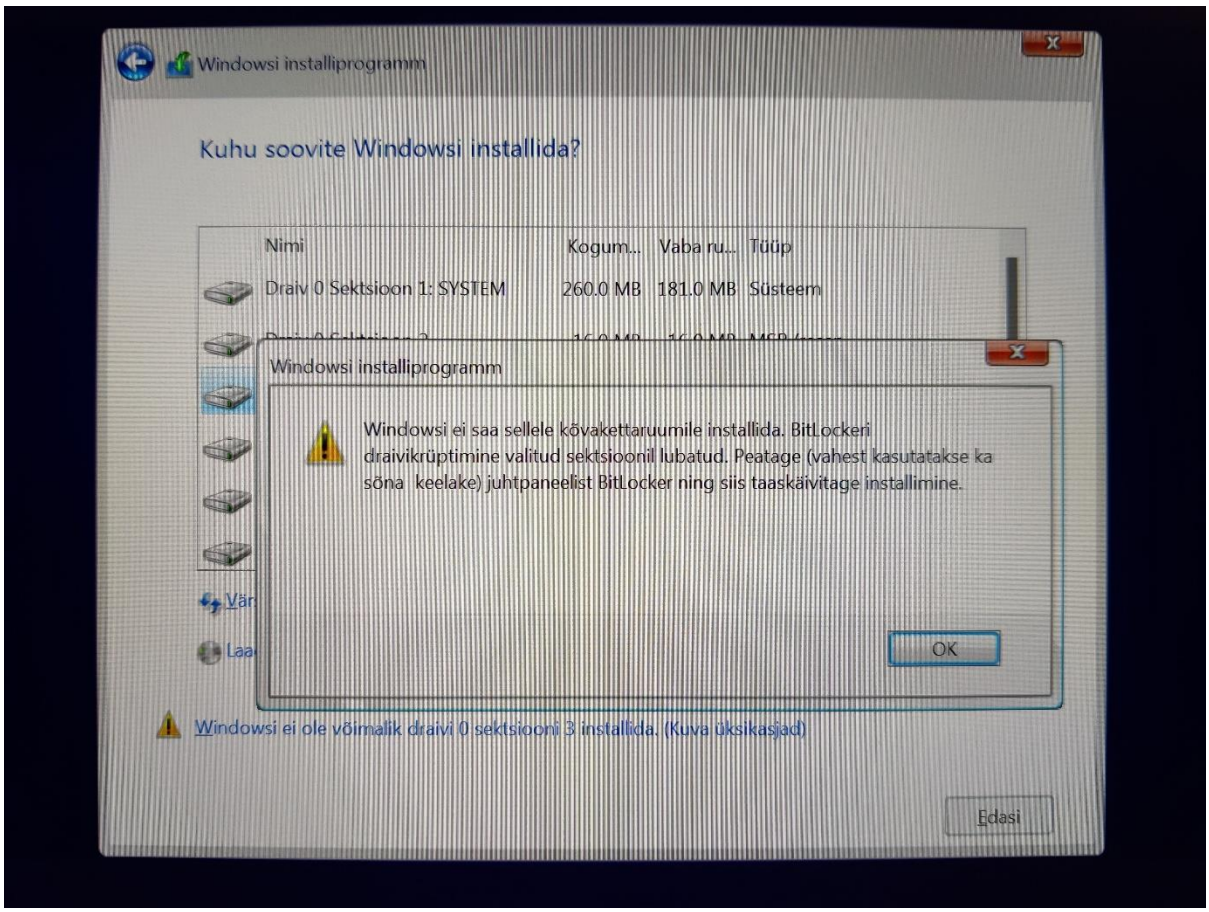
Parameeter	**Võimalikud väärtused**	**Funktsionaalsuse selgitus**	**Vaikeväärtus**
TPM Specification Version	Fikseeritud 2.0 väärtus	Turbeprotsessori spetsifikatsiooni versioon	2.0
TPM Device	Available	Turbeprotsessor saadaval ning sisse lülitatud süsteemi platvormi jaoks	Available
	Hidden	Turbeprotsessor peidetud süsteemi platvormile	
TPM State	Märkeruut märgitud/ei ole märgitud	Kui märkeruut on valitud, siis operatsioonisüsteem saab turbeprotsessorit kasutada ja võtta omaniku õigused.	Märgitud
Clear TPM	No	Turbeprotsessorit ei tühjendata	No
	On next boot	Järgmisel käivitusel tühjendatakse turbeprotsessor. Peale tühjendamist muudetakse vaikeväärtus tagasi *No*	
TPM Activation Policy	F1 to boot	Juhul kui TPM seadeid on uuendatud, siis kasutajale kuvatakse käivitamisel vastav teade ning seadme käivitamiseks ja muudatuste kinnitamiseks tuleb vajutada F1 klahvil	Allow user to reject
	Allow user to reject	Juhul kui TPM seadeid on uuendatud, siis kasutajale kuvatakse käivitamise vastav teade. Kasutajal on võimalus muudatus tagasi lükata või seade käivitada.	
	No prompts	Kasutajale ei kuvata TPM seadmete uuendamise kohta infot. Vajalik siis, kui on vaja paljusid süsteeme eemalt korraga uuendada.	

TPM ja Bitlocker praktikas

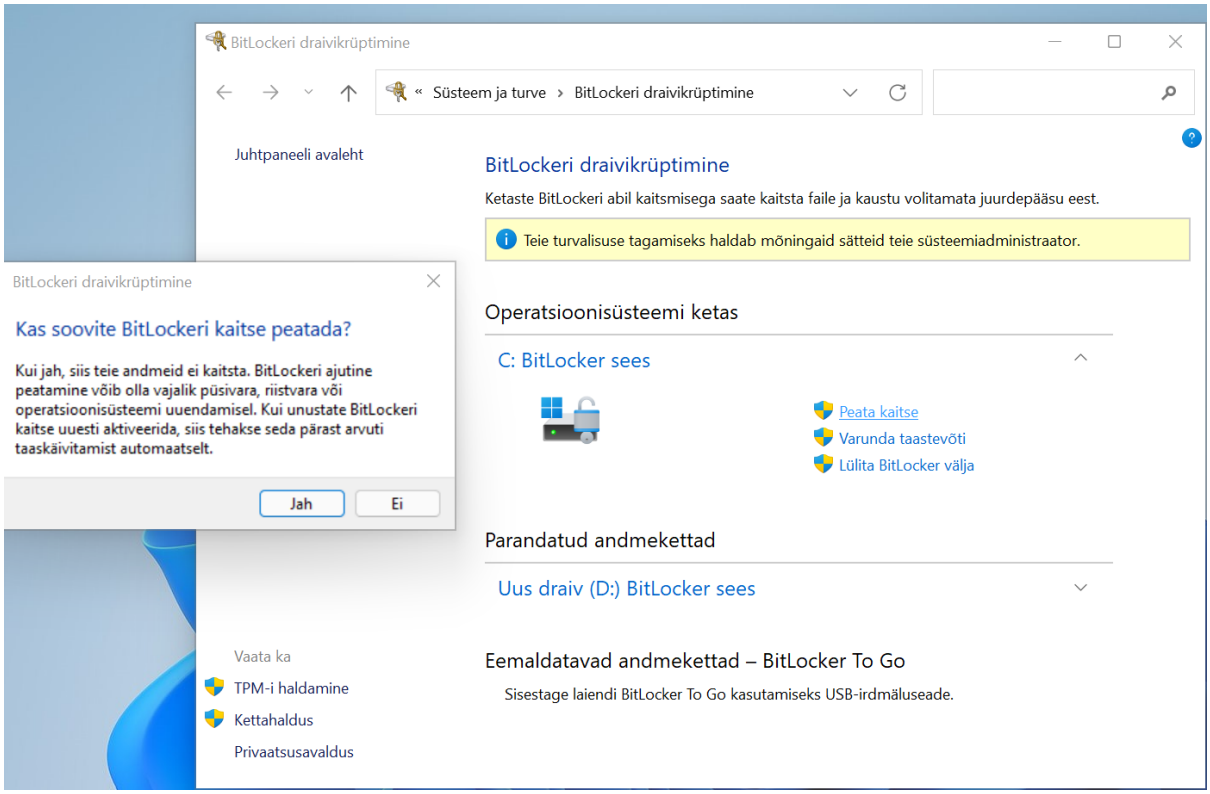
Antud peatükk katab tavakasutaja jaoks BitLockeri funktsionaalsuse praktikas. BitLockeril on palju erinevaid lisafunktsionaalsusi ning seda on võimalik erinevalt seadistada ja rakendada olemasolevat funktsionaalsust. Kõike seda saab huvi korra lugeda Microsofti BitLockeri ülevaatest [53]. Windows 10 ja Windows 11 operatsioonisüsteemides BitLockeri seadistamisel ja kasutamisel tavakasutaja jaoks antud töös erinevusi ei ilmnenud.

Kui Windowsi operatsioonisüsteemis on seadistatud Microsofti konto, siis HP Elitebookil on BitLocker vaikimisi eelseadistatud. Nagu BitLockeriga seotud peatükis 3.3 mainitud, siis tuleb BitLockeri sisse lülitamiseks see sellisel juhul lihtsalt aktiveerida. Aktiveerimise protsessi (lisa 5) järgselt on ketas krüpteeritud ja kaitstud. Kasutajamugavuse poolest on HP Elitebooki uue ketta krüpteerimine äärmiselt mugav ja kiire – kogu protsess (lisa 5) võttis aega alla minuti. Kuna BitLockeri seadistamine on tehtud nii kasutajasõbralikuks, siis see on väga sobiv turbefunktsionaalsus ka tavakasutajale, kes võib sattuda nii varguse ohvriks kui ka seadme lihtsalt kaotada.

Kui HP Elitebookil on BitLocker seadistatud ning aktiivne kogu ketta ulatuses, siis lisaks operatsioonisüsteemi olemasoleva kõrvale installeerida niisama lihtsalt ei ole võimalik (pilt 15). Selleks, et seda teha, on BitLockeril olemas lisafunktsioon „Peata kaitse“ (pilt 16), mis võimaldab püsivara, riistvara või operatsioonisüsteemi muudatusi teha. BitLockeri kaitse taastatakse automaatselt pärast seadme taaskäivitamist.

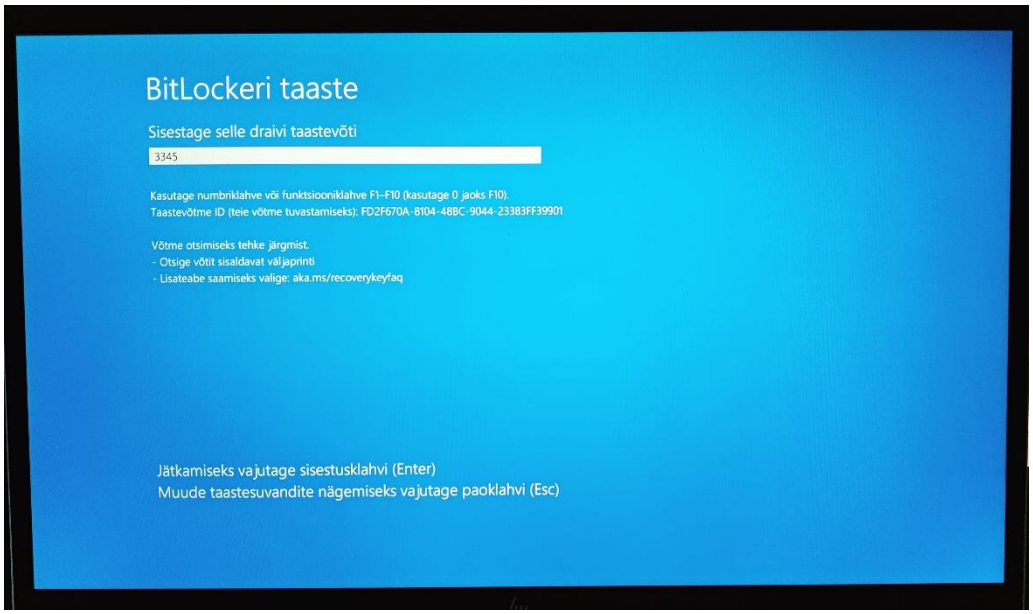


Pilt 15. Windowsi installprogrammi dialoogiaken, kui BitLockeriga kaitstud kettale üritatakse installida uut operatsioonisüsteemi



Pilt 16. BitLockeri kaitse peatamine

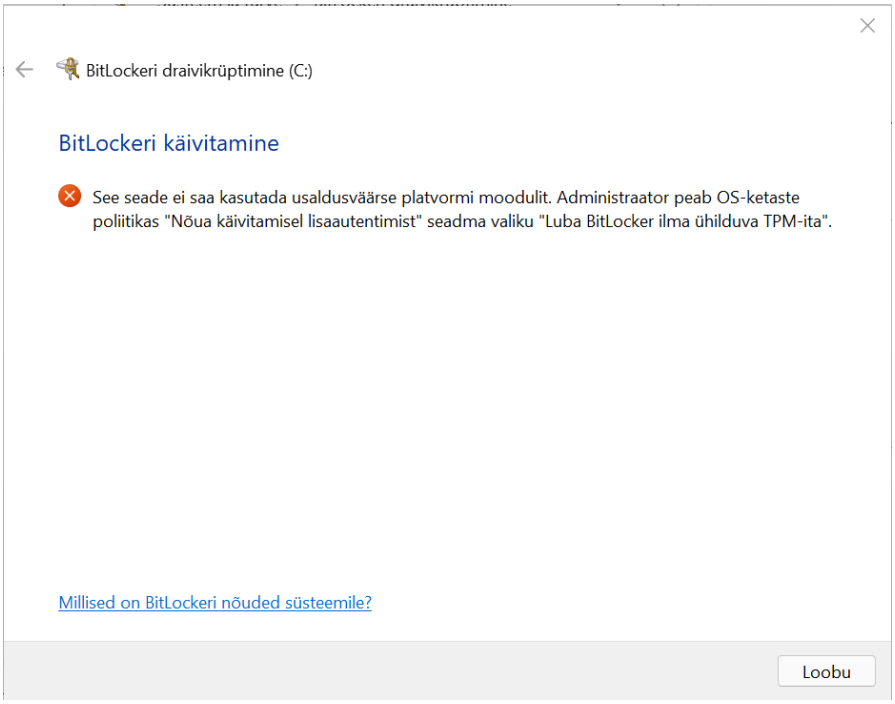
Kui BitLocker on sisse lülitatud seadmel, kus TPM on aktiivne, siis igasuguse turbeprotsessoriga manipuleerimise (ja ka teiste püsivaraliideses seadete muutmise) järgselt nõuab süsteem BitLockeri taastevõtit (pilt 17).



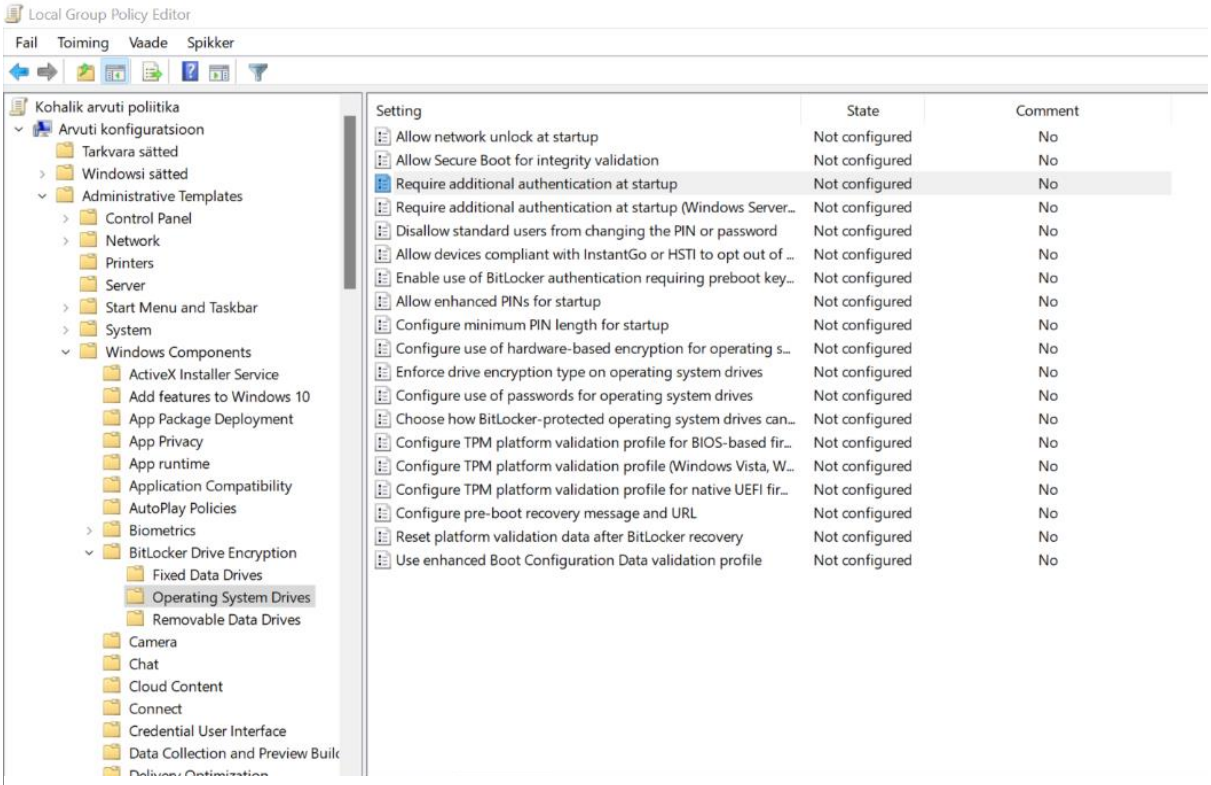
Pilt 17. BitLockeri taastevõtme sisestamise vaade

Kui BitLockeri krüptimine on seadistatud ning võti varundatud, siis ilma lisaturbepoliitikateta piisab kettal olevatele andmetele ligipääsemiseks seadmesse sisse logimisest Windows Hello kaudu. Selline ainulogimine muudab kogu BitLockeri ketta krüpteerimise kasutamise tavakasutaja jaoks mugavaks ja kasutajasõbralikuks.

HP Elitebook 840 G8 seadmel testiti lisaks aktiivse turbeprotsessoriga BitLockeri aktiveerimisele ja kasutusele, ka BitLockeri ketta krüpteerimist siis kui turbeprotsessor on välja lülitatud. Seda niisama lihtsalt teha ei ole võimalik (pilt 18) ja vajab lisaseadistust (pilt 19).

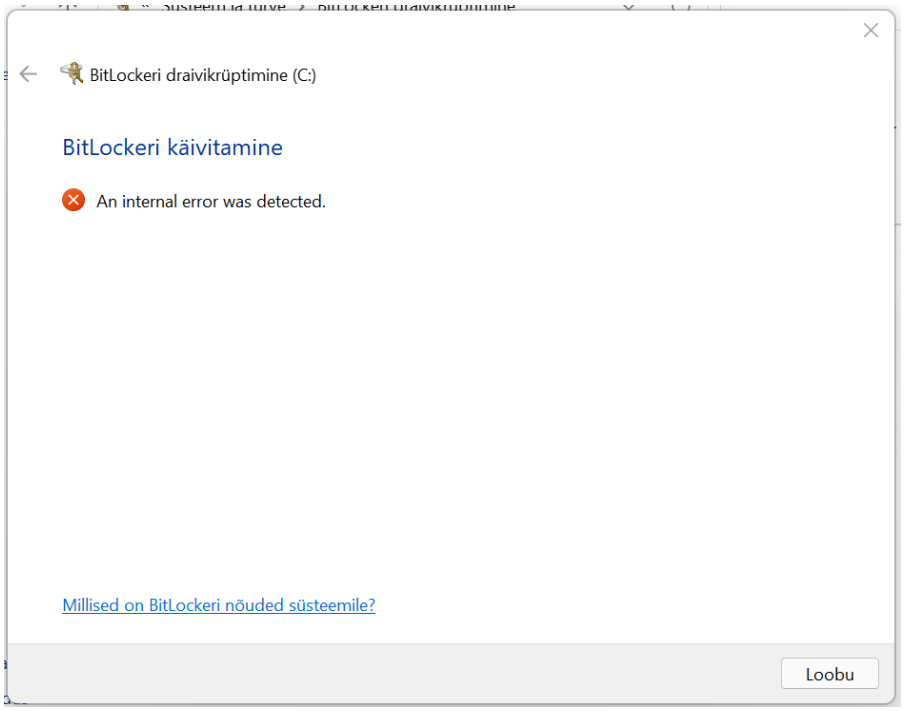


Pilt 18. BitLockeri käivitamisel kuvatav teade, kui turbeprotsessorit pole



Pilt 19. *Require additional authetication at startup* olek on vaja muuta "Enabled", selleks, et saaks BitLockerit seadistada turbeprotsessorita seadmes

Lisaks saab välja tuua, et HP Elitebookil tekkis BitLockeri sisse lülitamisel ootamatu tõrge (pilt 20), kui turbeprotsessor on küll saadaval, kuid operatsioonisüsteemi omaniku õigused puuduvad (*TPM State* UEFI püsivaraliideses märkimata).



Pilt 20. BitLockeri käivitamisel esineb ootamatu tõrge, kui turbeprotsessor on sees aga operatsioonisüsteemil omaniku õigused turbeprotsessori üle puuduvad

BitLockeri kasutamine on väga mugavaks tehtud just siis, kui seadmel on turbeprotsessor aktiivne. Seega tavakasutajal kindlasti tasub võtta see mõni minut aega, et BitLockeri ketta krüpteerimine sisse lülitada.

TPM ja Windows Hello praktikas

Windows Hello seadistamiseks on vaja HP Elitebookis läbida peatükis 1.2 selgitatud seadme registreerimise protsess. Esimene võimalus selleks on kasutajal siis, kui toimub Windowsi installeerimise järgselt operatsioonisüsteemi häälestamine. Antud töö raames oli eelduseks, et seade häälestatakse või on häälestatud isiklikuks kasutamiseks (Windowsi häälestamisel valik „Isiklikuks kasutamiseks seadistamine“). Hiljem on võimalik Windows Hello raamistiku sisselogimissuvandeid seadistada operatsioonisüsteemi rakendustest.

Kuna Microsofti enda dokumentatsioon Windows Hello raamistiku ning erinevate kontode tüüpide korral on tavakasutaja jaoks ebaselge, siis üks antud peatüki praktilise osa eesmärkidest on välja selgitada, kuidas toimib raamistiku seadistamine tavakasutaja jaoks erinevate autentimise meetoditega ning milliste kontode ja autentimismeetodite puhul on võtmed turbeprotsessori poolt reaalselt turvatud.

Windowsi häälestamisprotsess on üles ehitatud nii, et lokaalse konto seadistamine on kasutaja jaoks ebamugav ja autori hinnangul pigem tüütu, sest muud sisselogimissuvandid ei ole Microsofti konto seadistamisega võrreldes nähtaval kohal ning mitmeid kordi on vaja valida ja kinnitada, et soovitakse ühenduseta kontot luua. Microsofti konto seadistamine on aga

operatsioonisüsteemi (nii Windows 10 kui ka Windows 11) häälestamisprotsessi loogiline osa. Seega on Microsofti konto seadistamine kasutaja jaoks mugavam lahendus, kui lokaalne konto.

Microsofti konto eelised lisaks seadistamise mugavusele on autori hinnangul operatsioonisüsteemi isikupärastamise, rakenduste ja muude selliste seadistuste (näiteks BitLockeri ketta krüpteerimine) taaste võimalus pärast operatsioonisüsteemi lähtestamist või uue seadme kasutusele võttu. Selle miinuseks võib aga lugeda seda, et need andmed võetakse serverist ning ka seade registreeritakse serveris. Lokaalse konto plussiks on autori hinnangul see, et seadme registreerimiseks pole vaja internetti ning andmeid ei saadeta Microsofti serverisse, mis tagab kasutajale privaatsuse ja anonüümsuse.

Nii lokaalse konto kui Microsofti konto korral on seadmel HP Elitebook 840 G8 võimalik seadistada järgnevad autentimisvõimalused:

1. Lokaalse konto või Microsofti konto parool
2. Piltparool (täpsem kirjeldus peatükis 1.2)
3. Windows Hello raamistiku autentimismeetodid:
    a. Näotuvastus
    b. Sõrmejäljetuvastus
    c. PIN kood
4. Turvavõti – USB, NFC seade või kiipkaart
5. Lokaalsekonto puhul ilma paroolita

Turvavõti on alternatiivne variant seadme registreerimiseks. Seda antud töös ei testitud, kuid teoreetiliselt on sellega võimalik kasutada ka HP Elitebooki NFC ning kiipkaardi mugavusfunktsionaalsust. NFC turvavõtme kasutamiseks tuleb selleks soetada lähiväljaside toega turvavõti. Erinevate Microsofti partnerite nimekirja leiab Microsofti dokumentatsioonist[14].

Nii lokaalse konto kui ka Microsofti konto puhul on võimalik HP Elitebookil seadistada Windows Hello raamistiku kõik autentimisviisid. Microsofti konto puhul on võimalik operatsioonisüsteemi rakenduses „Sätted“ sisselogimissuvandite alamenüüs teha lisasätete alt valik „Turvalisuse parandamiseks lubage selles seadmes Microsofti kontode jaoks ainult Windows Hello sisselogimine“. Selle valiku korral kuvatakse seadme käivitamisel sisselogimise kuval vaid Windows Hello raamistiku autentimisviisid. See teeb seadme turvalisemaks, sest sümmeetriliselt krüpteeritud parooli ega ka piltparooli valikus ei ole, mida oleks võimalik jõuründe meetodil murda.

Selleks, et teada saada kas HP Elitebooki seadmel mõlema konto puhul on näotuvastus, sõrmejäljetuvastus ja PIN turbeprotsessori poolt kaitstud, seadistati kõigepealt kõik kolm tuvastusmeetodit. Seejärel manipuleeriti turbeprotsessoriga – tühjendati turbeprotsessorit, lülitati see välja ning võeti operatsioonisüsteemilt omaniku õigused. Selle tulemusena selgus, et mõlema konto, nii lokaalse kui ka Microsofti konto puhul, ei saa Windows Hello raamistiku autentimismeetodid enam kasutada ja järelikult on need turbeprotsessori poolt kaitstud. Edasises PIN koodi lähtestamisprotsessis esineb ootamatuid tõrkeid ning autori hinnangul on see protsess vigane (osa vigu esineb ka Windows 10 kui protsess ise on stabiilsem). Eriti esineb tõrkeid siis,

[14] https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-fido2-hardware-vendor

kui kasutusel on Microsofti konto ning eespool mainitud lisasäte, Windows Hello raamistikuga sisselogimise kohta, on sisse lülitatud. Mitmete katsete järel õnnestus siiski PIN kood lähtestada kasutades Microsofti kontot. Kui aga tegemist on lokaalse kontoga siis saab kasutaja alternatiivina logida sisse parooliga või piltparooliga. Biomeetriliste andmeid eraldi lähtestama ei pea, nendega saab sisse logida kui PIN kood on edukalt lähtestatud.

Olenemata, kuidas kasutaja seadme registreerib ja mis sisselogimissuvandid on kasutamiseks seadistatud, kuvatakse Windows 11 operatsioonisüsteemi Windowsi turbe rakenduses „Kontokaitse“ alamenüüs teade: „Sekkumine pole vajalik“. Autori hinnangul on see teave kasutaja jaoks eksitav ning see võiks olla kasutaja informeerimise jaoks täiustatud, arvestades, et Windows 11 on arendatud täisusaldamatuse turbepoliitikal.

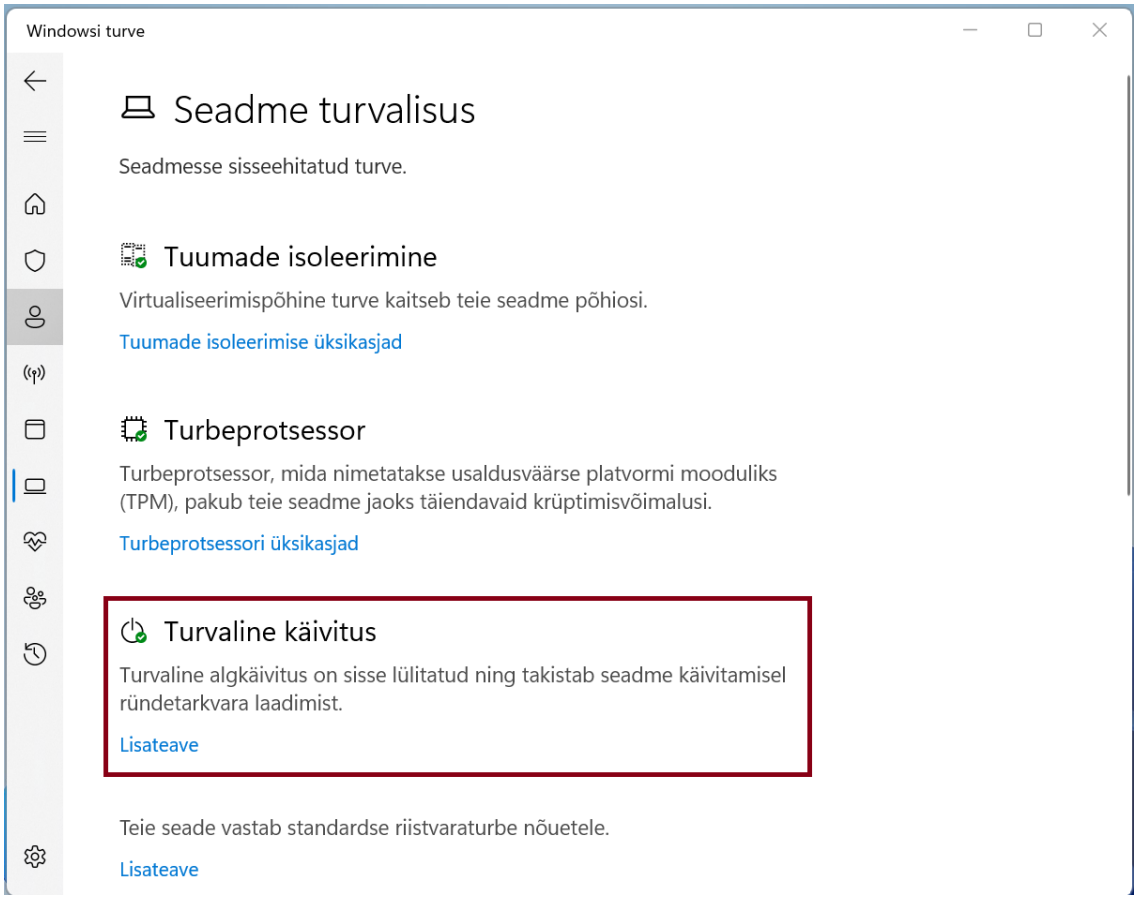
Teoreetiliselt on kõige turvalisem meetod autori hinnangul kasutada Microsofti kontoga Windows Hello raamistiku, ilma lisavõimalusi (parool ja piltparool) lisamata. Sellisel juhul ei ole võimalik sümmeetrilist parooli lihtsalt jõuründega ära arvata. Samas Windows 11 esinevate tõrgete tõttu autor seda hetkel veel ei soovita. Windows 11 on veel üsna värske operatsioonisüsteem ja suure tõenäosusega versioonitäienditega antud vead ka parandatakse, seega tulevikus on see tavakasutaja jaoks sobiv variant. Kõige ebaturvalisem variant on seadistada lokaalne konto ilma paroolita, mis tähendab seda, et seadme kasutamiseks pole vaja kasutajal end autentida. Seadme käivitamise järgselt on ligipääs andmetele ja operatsioonisüsteemi rakendustele olemas ning sisselogimiskuva kasutajale ei kuvata.

5.3 Turvaline käivitus

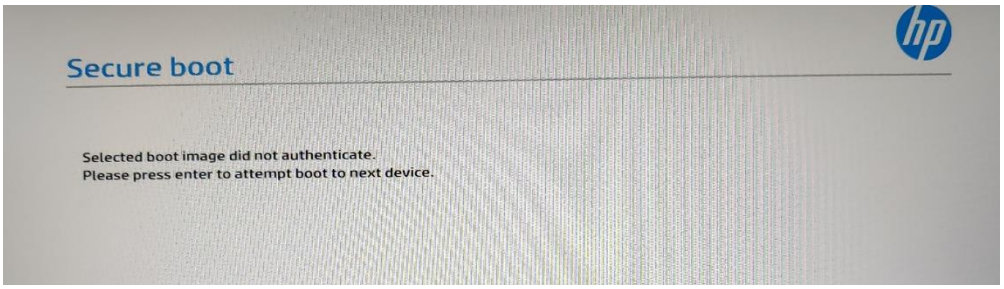
Turvaline käivitus on sarnaselt turbeprotsessorile ja virtualiseerimispõhisele turvalisusele vaikimisi sisse lülitatud mõlemas Windowsi versioonis. Windowsi turbe rakenduses kuvatakse kasutajale turvalise käivituse kohta infoteade (pilt 21). Välja- ja sisselülitamiseks on kasutajal võimalus kasutada UEFI püsivara liidesest (pilt 3). Kui kasutaja seda teha soovib, tuleks hinnata kas see on päriselt vajalik, kuna turvalise käivituse väljalülitamine muudab süsteemi käivitamisel pahatahtliku koodi suhtes haavatavaks.

UEFI püsivaraliidesest on turvalist käivitust võimalik välja ja sisse lülitada Security vahekaardilt Secure Boot Configuration alamenüüst. Seal samas kuvatakse kasutajale ka turvalise käivituse võtmete haldamise sätteid Secure Boot Key Management kategoorias (pilt 3). Kui kasutaja ei taha mingil põhjusel tootja võtmeid kasutada või on vaja süsteemi lisada kohandatud võtmeid (näiteks Linuxi operatsioonisüsteemi pildi jaoks), siis on võimalik seda teha just sellest alamosast. Kohandatud turvalise käivitamise võtmete kohta on võimalik lugeda täpsemalt tootja enda juhendist [54].

Nagu neljandas peatükis mainitud, siis turvaline käivitus on standard, mille eesmärk on tagada, et seade laeb käivitades ainult usaldusväärset tarkvara. Järgmist sammu alglaadimises ei tehta enne kui eelnev samm on hinnatud ohutuks. Juhul kui HP Elitebookil üritada sellist tarkvara käivitada, siis kuvatakse kasutajale vastav teade signatuuri mitte vastavuse kohta ning protsessi jätkamine ei ole võimalik (pilt 22). Käesoleval seadmel testiti seda buuditava seadmega, millel oli Kali Linux operatsioonisüsteem.



Pilt 21. Turvalise käivituse info rakenduses Windowsi turve



Pilt 22. Turvalise alglaadimise teade, kui käivitada mitte vastava signatuuriga tarkvara (näiteks Kali Linux operatsioonisüsteem)

6 Järeldused

Töö praktilises osas selgus, et kõik oluline turbelahendustega seotud info on kasutajale kuvatud Windows turbe rakenduses ning vajadusel ka rakenduses Süsteemiteave. Windows 10 ja Windows 11 kui versioonitäiendi korral kuvatakse HP Elitebook 840 G8 seadmes Windowsi turbe rakenduses kasutajale üldistav teade „Teie seade vastab standardse riistvaraturbe nõuetele". Windows 11 puhta installi korral kuvatakse samas kohas teade: „Teie seade vastab täiustatud riistvaraturbe nõuetele".

Eelnevast saab järeldada, et seadmel HP Elitebook 840 G8 puhul on tootja kõik olulised ja Windows 11 jaoks vajalikud riistvara turbefunktsionaalsused vaikeväärtustena sisse lülitanud. Kasutajal endal on võimalik operatsioonisüsteemi kasutajaliidese kaudu mõjutada vaid osa turbetehnoloogiaid. Teadlikumal tavakasutajal on kontroll siiski turbetehnoloogiate üle olemas ja seadeid on võimalik muuta UEFI püsivaraliidesest. Kuna kasutaja jaoks on sisuliselt kõik olulised turbefunktsionaalsused sisse lülitatud või eelseadistatud, ei muutu seadme kasutamine ebamugavaks ega tüütuks, vaid on just mugav ning mis kõige olulisem – turvaline. Tabel 4 võtab peatükis 7 kajastatud turbetehnoloogilised funktsionaalsused praktikas kokku.

Tabel 4. Turbetehnoloogiad HP Elitebook 840 G8 seadmel

Turbetehnoloogia		**Windows 10 ja Windows 11 kui versioonitäiend**	**Windows 11 puhas install**	**Seadistus**
Turbeprotsessor		Sisse lülitatud ja omaniku õigused operatsioonisüsteemile antud	Sisse lülitatud ja omaniku õigused operatsioonisüsteemile antud	Sisse-/väljalülitamine ja tühjendamine UEFI püsivaraliidesest; tühjendamine ka Windows turbe rakendusest
BitLocker		Eelseadistatud	Eelseadistatud	Operatsioonisüsteemi rakendustest
Windows Hello		Operatsioonisüsteemi häälestamisel, hiljem muudetav operatsioonisüsteemi rakendustest		
VBS (tuumade isoleerimine)	Mälu terviklus	Välja lülitatud	Sisse lülitatud	Sisse-/väljalülitamine Windowsi turbe rakendusest
	Mällupöörduse kaitse	Sisse lülitatud	Sisse lülitatud	Sisse-/väljalülitamine UEFI püsivaraliidesest
Turvaline käivitus		Sisse lülitatud	Sisse lülilitatud	Sisse-/väljalülitamine UEFI püsivaraliidesest

Samas tuleb tähele panna, et kuigi uue operatsioonisüsteemi Windows 11 tulekuga on kasutajate tähelepanu pööratud töös kajastatud turbetehnoloogiatele, on need tegelikult rakendatavad ka juba operatsioonisüsteemis Windows 10, kui seadmel endal on vajalikud riistvara turbefunktsionaalsused olemas. HP Elitebook 840 G8 puhul see nii ka on. Ainuke töös välja tulnud erinevus seisnes mälu tervikluse funktsioonis, mis on Windows 10 ning Windows 11 kui versioonitäiendi puhul välja lülitatud, kuid Windows 11 puhta installi puhul sisse lülitatud. Kuna see on aga kasutaja poolt kergesti muudetav otse Windows turbe rakenduses, siis see ei ole väga oluline erinevus.

Praktilises osas sai välja toodud ka tehnoloogiate kasutamisega seotud esinevaid probleeme või takistusi. Seega materjali läbi töötanud kasutaja teab nende algpõhjuseid, oskab neid oodata ning vajadusel ka lahendada (näiteks mälu terviklusega seotud draiverite ühildamine, turvalisel käivitusel signatuuri mittevastavus).

Microsofti meeskond väidab blogipostituses "Update on Windows 11 minimum system requirements" [55], et kombinatsioon uutest turvanõuetest vähendab pahavara 60% testitud seadmetes. See tuleb sellest, et Microsofti enda seadmetest saadud andmete põhjal raporteeriti 60% vähem aktiivset pahavara kui turbetehnoloogiad olid sisse lülitatud. Seega mitte ühegi töös kaetud turbetehnoloogia välja lülitamine ei ole autori hinnangul mõistlik. Veelgi enam, autori meelest on tark nii Windows 10 kui ka Windows 11 (versioonitäiendis) lülitada sisse mälu terviklus. Windows 11 puhta installi korral on see juba sisse lülitatud. Kui on aga vajadus turbetehnoloogiaid välja lülitada, siis antud töö läbinud kasutaja oskab arvestada võimalike riskidega ning teab, et seda on mõistlik teha vaid kontrollitud keskkonnas.

Kokkuvõtvalt saab järeldada, et HP Elitebook 840 G8 seadmel on riistvara turbetehnoloogiate kasutamine tehtud mugavaks ja kasutajast üsna sõltumatuks. Vajadusel saab aga kasutaja turbetehnoloogiate sätteid muuta kasutades selleks operatsioonisüsteemi seadme turvalisuse rakendust või seadme UEFI püsivaraliidest.

Windows 11 operatsioonisüsteemi vajadust tuleb aga kasutajal endal hinnata - ainuüksi riistvara turbelahenduste pärast see end ära ei õigusta, sest töös käsitletud ja uuritud tehnoloogiaid on ka Windows 10 operatsioonisüsteemis olemas. Saab väita, et operatsioonisüsteem Windows 11 on kasutaja jaoks täisusaldamatuse poliitikaga turvaline, kuid sarnaselt on võimalik kasutada ka Windows 10 operatsioonisüsteemi riistvaraliste turbetehnoloogiatega.

7 Kokkuvõte

Bakalaureuse töö üheks eesmärgiks oli koostada eestikeelne ülevaade tänapäevastest riistvaralistest turbelahendustest nagu turbeprotsessor, virtualiseerimispõhine turvalisus ning turvaline käivitus. Töö teine eesmärk oli kirjeldada HP Elitebook 840 G8 näitel nende turbetehnoloogiate praktilist kasutust operatsioonisüsteemis Windows 11.

Töö teoreetiline osa kattis mainitud turbetehnoloogiate tööpõhimõtete kirjeldust. Täpsemalt kirjeldati turbeprotsessoriga seotud raamistikku Windows Hello ning BitLockeri ketta krüpteerimist. Tänu materjalile on võimalik lugejal saada tervikpilt operatsioonisüsteemis Windows 11 kasutatavatest seadme turbetehnoloogiatest ning nende tööpõhimetest. Samuti tehnoloogiate kasutajamugavusest. Koostatud eestikeelne tehnoloogiate kirjeldus annab võimaluse tavakasutajal oma teadmisi täiendada ning lugejal oma töös vajadusel antud materjalidele toetuda.

Praktilise osa tulemusena tekkis kokkuvõttev materjal HP Elitebook 840 G8 näitel, mis on heaks aluseks Windowsi tavakasutaja jaoks, kes saab selle põhjal teha teadlikke otsuseid seoses seadmete enda ning nendega seotud riistvaraliste turbetehnoloogiatega. HP Elitebook 840 G8 seadmel on riistvara turbetehnoloogiate kasutamine tehtud tavakasutaja jaoks mugavaks ning kasutajast sõltumatuks, sest enamus töös mainitud tehnoloogiatest on vaikimisi sisse lülitatud juba seadme tootja ning operatsioonisüsteemi tarnija poolt. Samuti toodi praktilises osas välja ka turbetehnoloogiate kasutamisel esinevaid takistusi, seega lugeja teab nende algpõhjuseid ning oskab neid vajadusel lahendada. Lisaks järeldati praktilise osa tulemusena, et kuigi uue operatsioonisüsteemi Windows 11 nõuetega informeeritakse tavakasutajat riistvara turbetehnoloogiatest, on töös kajastatud turbetehnoloogiad olemas ka Windows 10 operatsioonisüsteemis, kui seade ise on toodetud riistvara turbetehnoloogia nõudeid silmas pidades. Seega kui värskelt turule tulnud Windows 11 tundub kasutajale liialt uuenduslik ja testimata, siis Microsofti vanemas operatsioonisüsteemis Windows 10 on sarnaselt võimalik kõiki tehnoloogiaid edukalt ja turvaliselt kasutada.

Selles töös on kaetud riistvaralised turbetehnoloogiad, mille eesmärk on kaitsta seadet ennast ning operatsioonisüsteemi eelset keskkonda. Kuna Windows 11 on arendatud täisusaldamatuse turbepoliitikal siis ehk on täiustatud selles töös kajastamata tarkvaralised turbelahendused külgrünnete ja reaalajas anomaaliate lahendamiseks. Sellised Windowsi turbetehnoloogiad on näiteks viiruse- ja ohutõrje, tulemüür ja võrgukaitse, rakenduse- ja brauseri turvasätted. Seega kuna töö katab vaid väikese osa kõikidest Windowsi turvalisusega seotud funktsioonidest, siis on see sobiv alus edasiseks uurimistööks ja miks mitte ka kirjeldatud turbetehnoloogiate täpsemaks analüüsiks.

8 Viidatud kirjandus

1. StatCounter Global Stats. [Veebileht]. (2022 veebruar). https://gs.statcounter.com/os-market-share/desktop/europe.
2. LH N. Windows 11's Security Push Puts Microsoft on a Collision Course. [Veebileht].; 2021 (2022 veebruar 2022). https://www.wired.com/story/windows-11-hardware-requirements-security/.
3. SJ VN. Windows 11: Just say no. [Veebileht].; 2021 (2022 veebruar 7). https://www.computerworld.com/article/3633630/windows-11-just-say-no.html.
4. K. G. Why I hate Windows 11 — here's what Microsoft needs to fix. [Veebileht].; 2021 (2022 veebruar 7). https://www.laptopmag.com/features/why-i-hate-windows-11.
5. M H. Windows 11 review: An unnecessary replacement for Windows 10. [Veebileht].; 2021 (2022 veebruar 7). https://www.pcworld.com/article/539183/windows-11-review-an-unnecessary-replacement-for-windows-10.html.
6. Microsoft Corporation. Täisusaldamatuse mudel – tänapäevane turbearhitektuur. [Veebileht]. (2022 jaanuar 5). https://www.microsoft.com/et-ee/security/business/zero-trust.
7. Microsoft Corporation. Windows 11 specs and system requirements. [Veebileht]. (2022 jaanuar 3). https://www.microsoft.com/en-us/windows/windows-11-specifications.
8. Justiitsministeerium. Kuritegevus Eestis 2020 - Küberkuriteod. [Veebileht].; 2020 (2022 03 03). https://www.kriminaalpoliitika.ee/kuritegevus2020/kuberkuriteod/.
9. Riigi Infosüsteemi Amet. Trendid ja tähelepanekud küberruumis – IV kvartal 2021. [Veebileht].; 2021 (2022 03 03). https://www.ria.ee/et/uudised/trendid-ja-tahelepanekud-kuberruumis-iv-kvartal-2021.html.
10. BR RW. UEFI Secure Boot in Modern Computer Security Solutions. [Veebileht].; 2013 (2022 jaanuar 27). https://media.kasperskycontenthub.com/wp-content/uploads/sites/63/2014/06/21032725/UEFI_Secure_Boot_in_Modern_Computer_Security_Solutions_2013.pdf.
11. The Trusted Computing Group. Iso/iec 11889-1:2015. [Veebileht].; 2021 (2022 jaanuar 5). https://www.iso.org/standard/66510.html.
12. The Trusted Computing Group. TPM 2.0 A Brief Introduction. [Veebileht].; 2019 (2022 jaanuar 26). https://trustedcomputinggroup.org/wp-content/uploads/2019_TCG_TPM2_BriefOverview_DR02web.pdf.
13. Microsoft Corporation. TPM recommendations. [Veebileht]. (2022 jaanuar 5). https://docs.microsoft.com/en-us/windows/security/information-protection/tpm/tpm-recommendations.
14. Microsoft Corporation. Trusted Platform Module (TPM) fundamentals (Windows) - Windows security. [Veebileht]. (2022 jaanuar 5). https://docs.microsoft.com/en-us/windows/security/information-protection/tpm/tpm-fundamentals.

15. Arthur W CDGK. A Practical Guide to TPM 20: Using the New Trusted Platform Module in the New Age of Security. [Veebileht].; 2015 (2022 jaanuar 5). https://doi.org/10.1007/978-1-4302-6584-9_3.
16. Microsoft Corporation. Trusted plaform module (TPM) 2.0. [Veebileht]. (2022 jaanuar 26). https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-tpm.
17. Microsoft Corporation. Trusted Platform Module technology overview. [Veebileht]. (2022 jaanuar 5). https://docs.microsoft.com/en-us/windows/security/information-protection/tpm/trusted-platform-module-overview.
18. Microsoft Corporation. How Windows uses the TPM - Windows security. [Veebileht]. (2022 jaanuar 5). https://docs.microsoft.com/en-us/windows/security/information-protection/tpm/how-windows-uses-the-tpm.
19. Micrisoft Corporation. Device health attestation. [Veebileht]. (2022 jaanuar 26). https://docs.microsoft.com/en-us/windows-server/security/device-health-attestation.
20. A S. A breakthrough year for passwordless technology. [Veebileht].; 2020 (2022 jaanuar 26). https://www.microsoft.com/security/blog/2020/12/17/a-breakthrough-year-for-passwordless-technology/.
21. Microsoft Corporation. Overview of BitLocker Device Encryption in Windows. [Veebileht]. (2022 jaanuar 5). https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-device-encryption-overview-windows-10.
22. Microsoft Corporation. Windows Hello for Business overview. [Veebileht]. (2022 jaanuar 5). https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-overview.
23. FIDO Alliance. FIDO2: Moving the world beyond passwords using WebAuthn & CTAP. [Veebileht].; 2019 (2022 jaanuar 5). https://fidoalliance.org/fido2/.
24. W3C. Web Authentication: An API for accessing Public Key Credentials. [Veebileht].; 2021 (2022 veebruar 2). https://www.w3.org/TR/webauthn-2/.
25. Microsoft Corporation. How Windows Hello for Business works - Windows security. [Veebileht]. (2022 jaanuar 5). https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-how-it-works.
26. Microsoft Corporation. How SSO to on-premises resources works on Azure AD joined devices. [Veebileht]. (2022 jaanuar 27). https://docs.microsoft.com/en-us/azure/active-directory/devices/azuread-join-sso.
27. Ejin Kim, Hyoung-Kee Choi. Security Analysis and Bypass User Authentication Bound to Device of Windows Hello in the Wild. [Veebileht].; 2021 (2022 jaanuar 26). https://downloads.hindawi.com/journals/scn/2021/6245306.pdf.
28. Microsoft Corporation. Windows Hello for Business documentation. [Veebileht]. (2022 jaanuar 27). https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/.

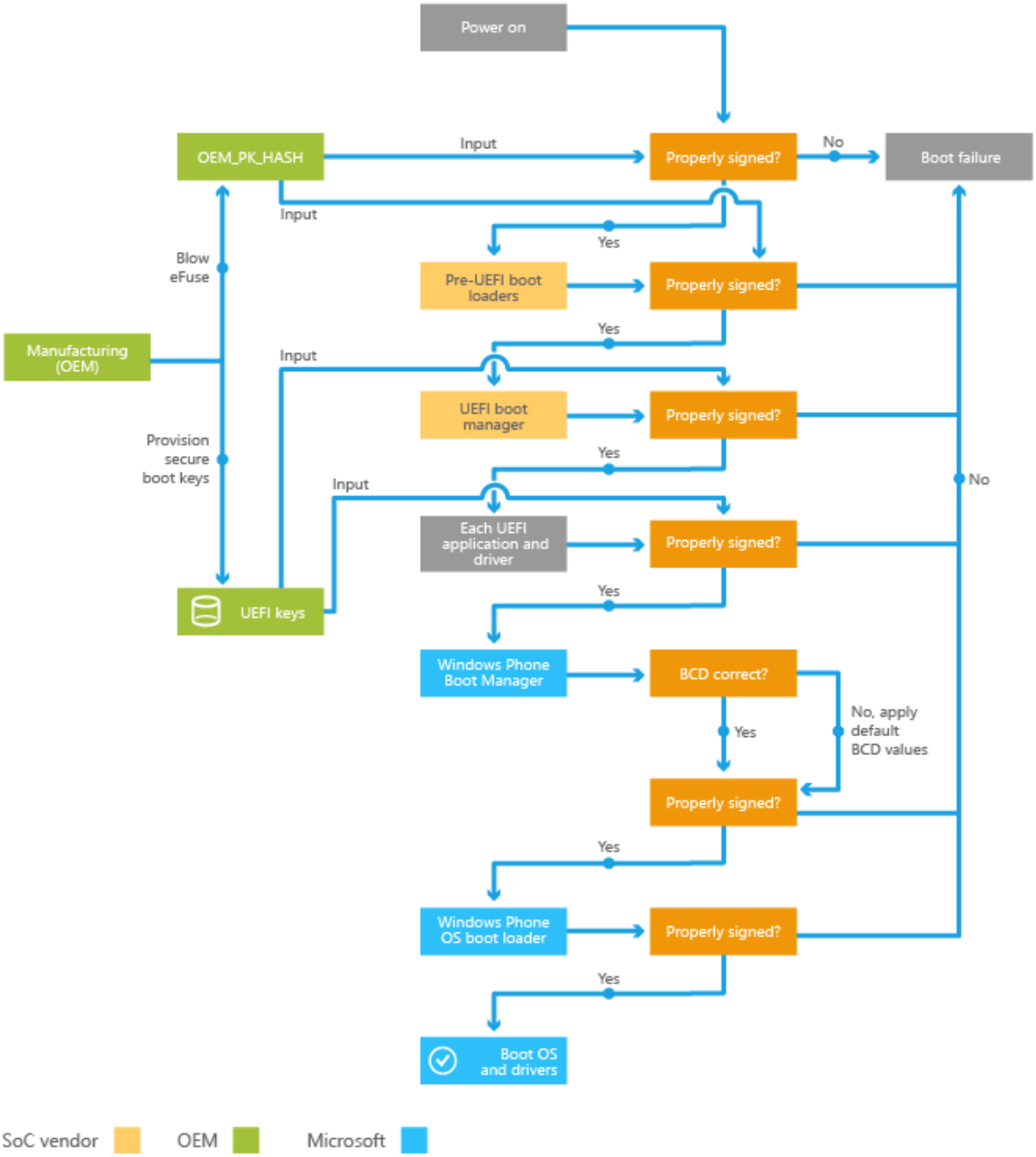
29. Microsoft Corporation. Planning a Windows Hello for Business deployment. [Veebileht]. (2022 jaanuar 27). https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-planning-guide.
30. Microsoft Corporation. Why a PIN is better than a password. [Veebileht]. (2022 jaanuar 5). https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-why-pin-is-better-than-password.
31. Microsoft Corporation. Windows Hello biometrics in the enterprise. [Veebileht]. (2022 jaanuar 5). https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-biometrics-in-enterprise.
32. Microsoft Corporation. Windows Hello biometric requirements. [Veebileht]. (2022 jaanuar 27). https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/windows-hello-biometric-requirements.
33. Microsoft Corporation. Become a Microsoft-compatible FIDO2 security key vendor for sign-in to azu-re AD. [Veebileht]. (2022 jaanuar 27). https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-fido2-hardware-vendor.
34. Microsoft Corporation. Secure boot. [Veebileht]. (2022 jaanuar 5). https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-secure-boot.
35. gushiciku.cn. There's a Hole in the Boot. [Veebileht].; 2020 (2022 jaanuar 27). https://www.gushiciku.cn/pl/p3kS.
36. Microsoft Corporation. Virtualization-based security (VBS). [Veebileht]. (2022 jaanuar 5). https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-vbs.
37. Intel. Intel® VT: Intel® Virtualization Technology - what is Intel® VT?. [Veebileht]. (2022 jaanuar 17). https://www.intel.com/content/www/us/en/virtualization/virtualization-technology/intel-virtualization-technology.html.
38. AMD. Virtualization Solutions. [Veebileht]. (2022 jaanuar 17). https://www.amd.com/en/technologies/virtualization-solutions.
39. Microsoft Corporation. Windows processor requirements. [Veebileht]. (2022 jaanuar 17). https://docs.microsoft.com/en-us/windows-hardware/design/minimum/windows-processor-requirements.
40. Microsoft Corporation. Virtualization based security system resource protections. [Veebileht]. (2022 jaanuar 31). https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/vbs-resource-protections.
41. HP Support. HP EliteBook 840 G8 Notebook PC specifications. [Veebileht]. (2022 jaanuar 5). https://support.hp.com/ee-en/document/c06978058.
42. Infineon. OPTIGATM TPM SLB 9670 TPM2.0 Trusted Platform Module Data Sheet. [Veebileht].; 2018 (2022 jaanuar 31). https://www.infineon.com/dgdl/Infineon-SLB%209670VQ2.0-DataSheet-v01_04-EN.pdf?fileId=5546d4626fc1ce0b016fc78270350cd6.

43. Intel Corporation. Intel® Core™ i5-1135G7 Processor. [Veebileht]. (2022 veebruar 5). https://ark.intel.com/content/www/us/en/ark/products/208658/intel-core-i51135g7-processor-8m-cache-up-to-4-20-ghz.html.
44. HP PCs - secure Boot (windows 10). [Veebileht]. (2022 jaanuar 5). https://support.hp.com/lv-en/document/c04784866.
45. Microsoft Corporation. Device protection in Windows Security. [Veebileht]. (2022 jaanuar 5). https://support.microsoft.com/en-us/windows/device-protection-in-windows-security-afa11526-de57-b1c5-599f-3a4c6a61c5e2.
46. Microsoft Corporation. Policy CSP - DeviceGuard. [Veebileht]. (2022 jaanuar 17). https://docs.microsoft.com/en-us/windows/client-management/mdm/policy-csp-deviceguard.
47. Microsoft Corporation. Hypervisor-protected Code Integrity enablement. [Veebileht]. (2022 jaanuar 5). https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-hvci-enablement.
48. Microsoft Corporation. Disable Hyper-V to run virtualization software - Windows Client. [Veebileht]. (2022 jaanuar 17). https://docs.microsoft.com/en-us/troubleshoot/windows-client/application-management/virtualization-apps-not-work-with-hyper-v.
49. Microsoft Corporation. Kernel DMA Protection. [Veebileht]. (2022 veebruar 8). https://docs.microsoft.com/en-us/windows/security/information-protection/kernel-dma-protection-for-thunderbolt.
50. The Trusted Computing Group. TCG PC Client Physical Presence Interface Specification. [Veebileht]. (2022 veebruar 8). https://trustedcomputinggroup.org/resource/tcg-physical-presence-interface-specification/.
51. Microsoft Corporation. TPM Key Attestation. [Veebileht]. (2022 veebruar 8). https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/tpm-key-attestation.
52. Microsoft Corporation. Turvalisuse protsessori tõrkeotsing. [Veebileht]. (2022 jaanuar 26). https://support.microsoft.com/et-ee/windows/turvalisuse-protsessori-t%C3%B5rkeotsing-25e5020c-f763-4137-a395-aa869ac29402.
53. Microsoft Corporation. BitLocker. [Veebileht]. (2022 veebrua 8). https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview.
54. Hewlett-Packard Development Company. Secure Boot. [Veebileht].; 2017 (2022 veebruar 16). https://h10032.www1.hp.com/ctg/Manual/c05649759.
55. Microsoft Corporation. Update on Windows 11 minimum system requirements. [Veebileht].; 2021 (2022 jaanuar 5). https://blogs.windows.com/windows-insider/2021/06/28/update-on-windows-11-minimum-system-requirements/.
56. Microsoft Corporation. Secure boot and device encryption overview. [Veebileht]. (2022 jaanuar 27). https://docs.microsoft.com/en-us/windows-hardware/drivers/bringup/secure-boot-and-device-encryption-overview.
57. HP Support. HP Support. [Veebileht]. (2022 jaanuar 25). https://support.hp.com/.

58. Microsoft Corporation. Oluline edusamm paroolide kõrvaldamise teekonnal: FIDO2/WebAuthn on määratud soovituse kandidaadiks. [Veebileht].; 2018 (2022 jaanuar 24). https://www.microsoft.com/et-ee/microsoft-365/blog/2018/04/12/big-news-in-our-drive-to-eliminate-passwords-fido2-webauthn-reaches-candidate-recommendation-status.
59. Microsoft Corporation. How Windows uses the TPM - Windows security. [Veebileht]. (2022 jaanuar 27). https://docs.microsoft.com/en-us/windows/security/information-protection/tpm/how-windows-uses-the-tpm.
60. Infineon Technologies AG. SLB 9670VQ2.0. [Veebileht]. (2022 jaanuar 24). https://www.infineon.com/cms/en/product/security-smart-card-solutions/optiga-embedded-security-solutions/optiga-tpm/slb-9670vq2.0/.

Lisad

Lisa 1. Sündmuste jada seadme käivitamisel [56]



1. Seadme tootmise ajal loovad originaalseadmete tootjad turvalised signatuurandmebaasid (täpsemalt kirjeldatud peatükis “UEFI turvaline käivitus”).
2. Seadme käivitamisel algab UEFI eelsete signatuuride valideerimine vastu põhivara. Kui see kontroll õnnestub, siis UEFI alglaadimishaldur käivitatakse.

3. UEFI alglaadimishaldur laeb ning kontrollib iga UEFI rakenduse ja draiveri signatuuri. Kui kontroll ebaõnnestub, siis käivitusprotsess ebaõnnestub.
4. Kui alglaadimishaldur on edukalt käivitunud, kontrollib see, et alglaadimise seadistuste andmestik (BCD) on korrektsed. Kui ei ole, siis operatsioonisüsteem kasutab turvalise alglaadimise poliitikatest lähtuvaid korrektseid väärtusi ning ignoreerib teisi.
5. Alglaadimishaldur valideerib operatsioonisüsteemi alglaaduri ning laeb selle vaid siis, kui signatuur on korrektne.
6. Operatsioonisüsteemi alglaadur omakorda valideerib kõik käivituseks kriitilised draiverid enne nende ja tuuma laadimist. Sellest hetkest edasi on tuuma ülesanne valideerida draiverite ja rakenduste signatuurid enne nende laadimist.

Lisa 2. Varasemad Tartu Ülikooli arvutiteaduste instituudi poolt tudengitele laenutatud seadmed ja nende vastavus Windows 11 turbenõutele.

Seade	TC/HP Elitebook 840	HP Elitebook 840 G2	HP Elitebook 840 G3 NB
Ostuaeg	07.07.2014	19.06.2015	20.06.2016
Protsessor	i5-4200U Ei vasta Win11 turbetehnoloogia nõuetele	i5-5200U Ei vasta Win11 turbetehnoloogia nõuetele	i5-6200U Ei vasta Win11
Turvaline käivitus	Olemas	Olemas	Olemas
TPM 2.0 [57]	Originaalis TPM 1.2 uuendusega võimalik 2.0	TPM 2.0	Originaalis TPM 1.2 uuendusega TPM 2.0
Vastab Win11 nõuetele	Ei vasta	Ei vasta	Ei vasta
Lisainfo	1x8GB RAM 256GB SED SSD ID kaardi lugeja a/b/g/n + BT4.0 3C 50WHr aku altvalgustusega klaviatuur SWE/FI Windows 8 64-bit	8GB RAM 256GB SSD a/b/g/n - BT4.0 altvalgustusega SWE/FI klaviatuur 3C 50Whr aku W8.1ML	16GB RAM 256GB M.2 SSD Backlit SWE/FI klaviatuur wireless AC BT4.2 W10H64

Seade	HP EliteBook 840 G4	HP EliteBook 840 G5	HP EliteBook 840 G5
Ostuaeg	26.06.2017	31.05.2018	30.04.2019
Protsessor	i5-7200U Ei vasta Win 11 turbetehnoloogia nõuetele	i5-8250U Vastab Win11 turbetehnoloogia nõuetele	i5-8250U Vastab Win11 turbetehnoloogia nõuetele
Turvaline käivitus	Olemas	Olemas	Olemas
TPM 2.0 [57]	TPM 2.0	TPM 2.0 Infineon SLB9670	TPM 2.0 Infineon SLB9670

Vastab Win11 nõuetele	Ei vasta	Vastab	Vastab
Lisainfo	14" FHD 16GB DDR4 (1x16) 256GB PCIe NVMe SSD Intel ac + BT4.2 Backlit SWE/FI kla-viatuur W10H64	14'' FHD IPS 16GB DDR4 2400 256GB PCIe NVMe SSD ID-kaardi lugeja SWE/FI backlit kla-viatuur Intel ac + BT4.2 W10H64	14" FHD IPS 16GB DDR4 (1DIMM) 256GB PCIe NVMe SSD ID-kaardi lugeja Intel AC, BT4.2, WWAN ready Backlit SWE/FI kla-viatuur W10H64

Seade	HP Elitebook 840 G6 NB	HP Elitebook 840 G8
Ostuaeg	01.07.2020	01.07.2021
Protsessor	i5-8265U Vastab Win11 turbe-tehnoloogia nõuetele	Core i5 1135G7 Vastab Win11 turbe-tehnoloogia nõuetele
Turvaline käivitus	Olemas	Olemas
TPM 2.0 [57]	TPM 2.0	TPM 2.0
Vastab Win11 nõuetele	Ei vasta	Vastab
Lisainfo	14" FHD i5-8265U 16GB DDR4 512GB PCIe NVMe SSD Intel 9560 ac + BT5 ID-kaardi lugeja Backlit SWE/FI kla-viatuur W10H64	Win 10 Pro 64-bit 16 GB RAM 512 GB SSD NVMe 14" IPS 1920 x 1080 (Full HD) @ 60 Hz Iris Xe Graphics NFC Bluetooth Wi-Fi - kbd: Pan Nordic

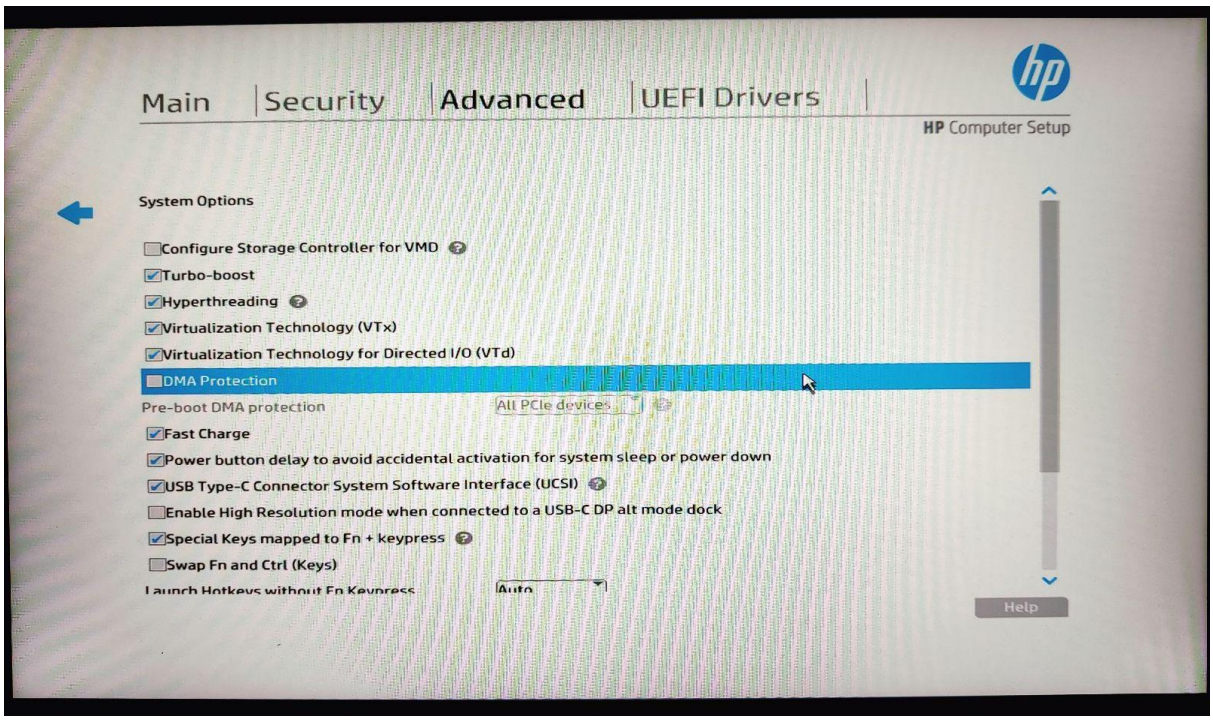
Lisa 3. Operatsioonisüsteemi Windows 10 installeerimisaegne Windows 11 jaoks riistvaraliste nõuete kontroll

a) Kui alustada Windows 10 installeerimisprotsessiga ja seade tegelikult vastab ka Windows 11 nõuetele, siis kuvatakse kasutajale võimalus valida operatsioonisüsteem Windows 11:

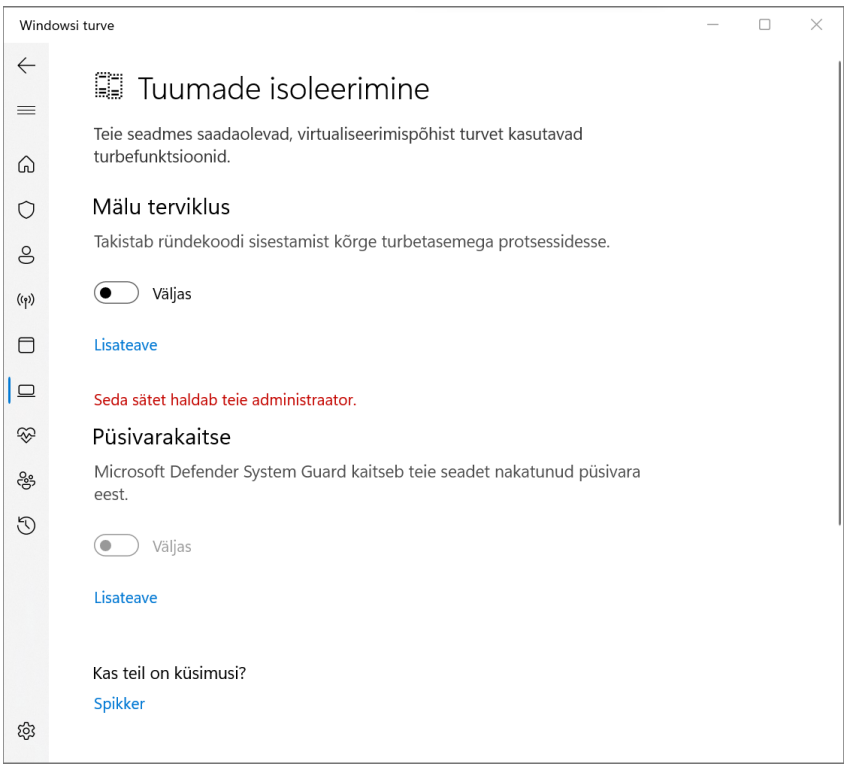
b) Kui kasutaja keeldub versioonitäiendusest, kuvatakse järgmise vaatena turunduslikku soovitust siiski Windows 11 proovida:

Lisa 4. Juhend mällupöörduse kaitse sisse ja välja lülitamiseks

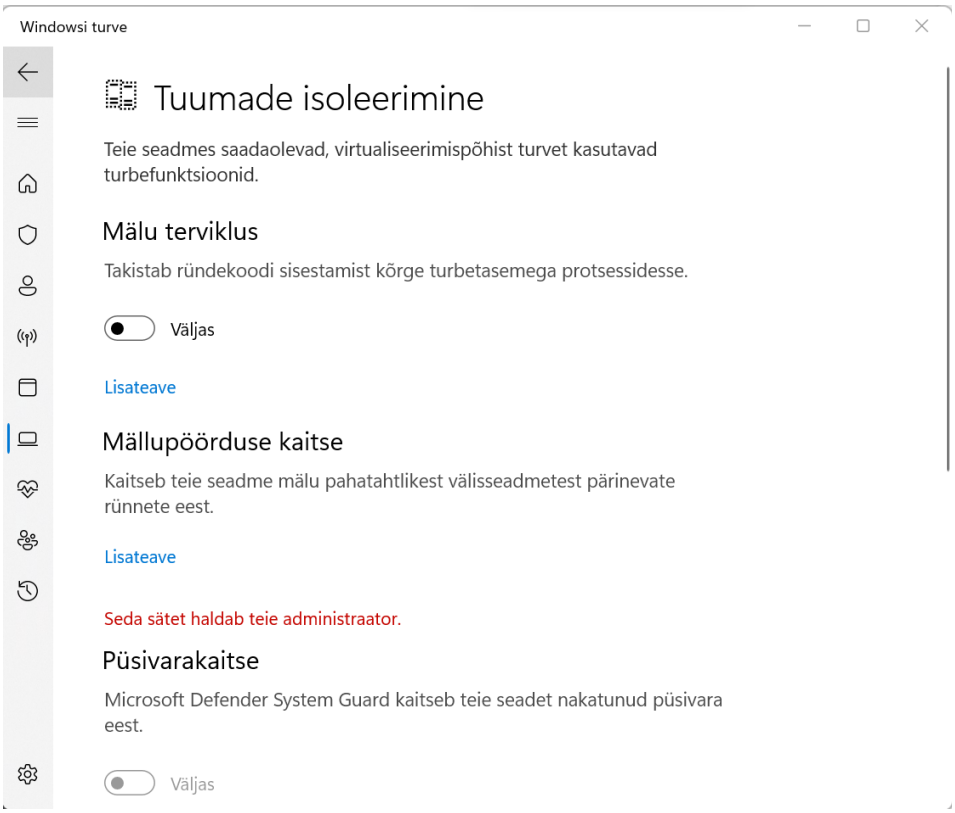
1. Kasutaja avab ühtse laiendatava püsivaraliidese (UEFI)
2. Edasi tuleb navigeerida menüüsse “Advanced”
3. Tuleb avada “System Options” alammenüü
4. Muuta vastavalt DMA Protections valik sisse või välja lülitatuks



Kui DMA Protection on välja lülitatud ei kuvata kasutajale Windows turbe rakenduses Mällupöörduse kaitse kohta infot:



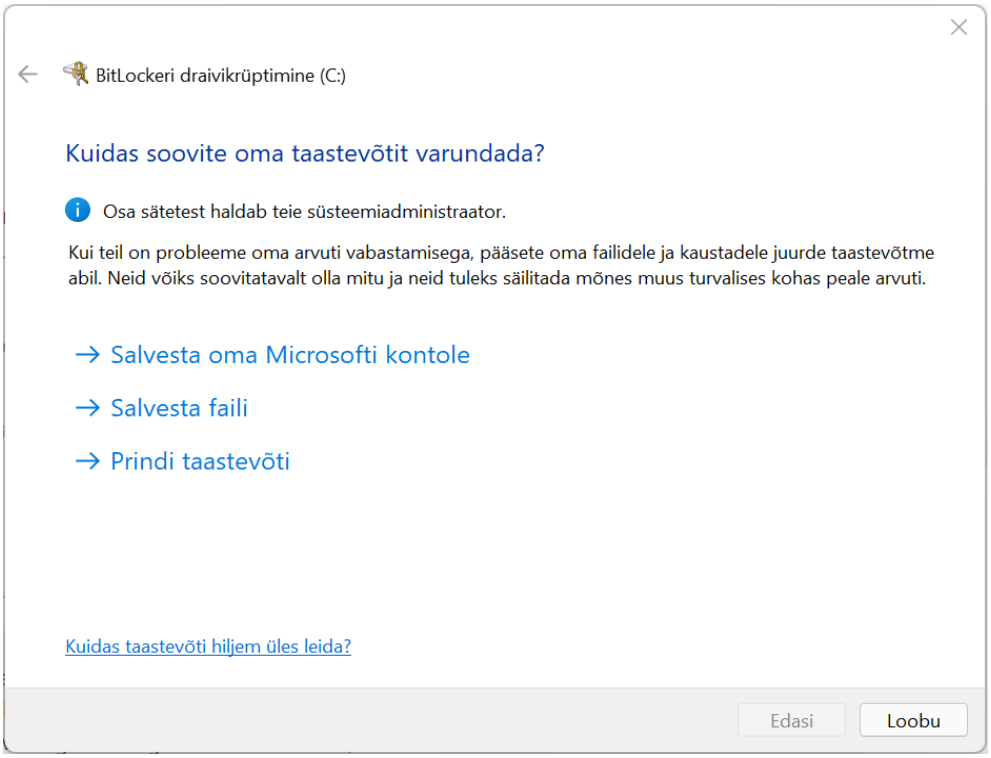
Kui DMA Protection on sisse lülitatud kuvatakse kasutajale Windows turbe rakenduses Mällupöörduse kaitse kohta infot:



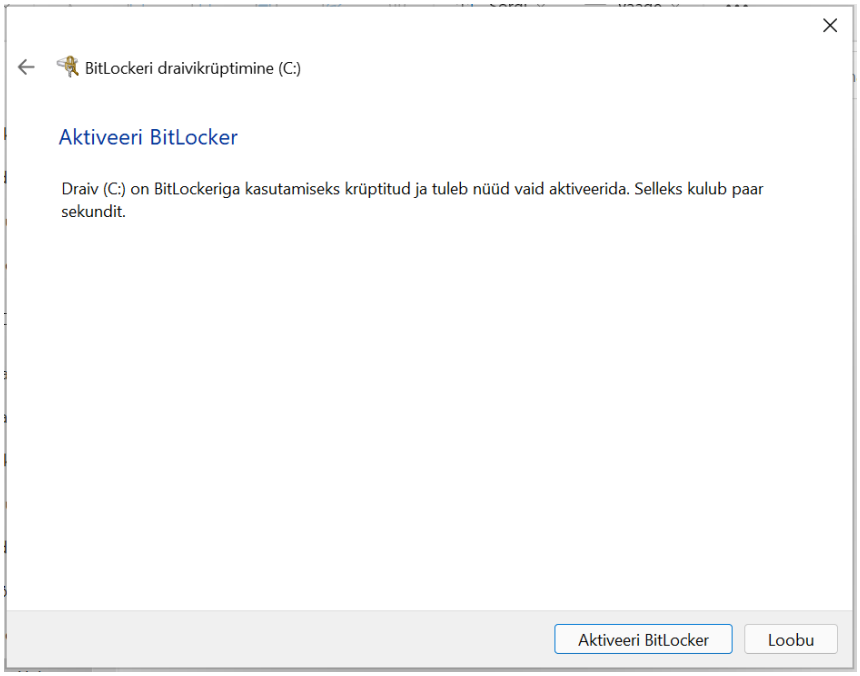
Lisa 5. BitLockeri ketta krüpteerimise seadistamise juhend ja kirjeldus

BitLockeri seadistamine kui seade on eelseadistatud (seade on autenditud Microsofti kasutajaga) BitLockeri kasutamiseks:

1. Krüpteerimiseks tuleb avada juhtpaneeli alt Süsteem ja turve ning sealt BitLockeri draivikrüptimine. Selles vaates vali "Lülita BitLocker sisse"
2. Järgmiseks tuleb valida kuidas soovite oma taastevõtit varundada. Valikus on kolm varianti: salvestamine Microsofti kontole, salvestamine faili ning taastevõtme printimine.

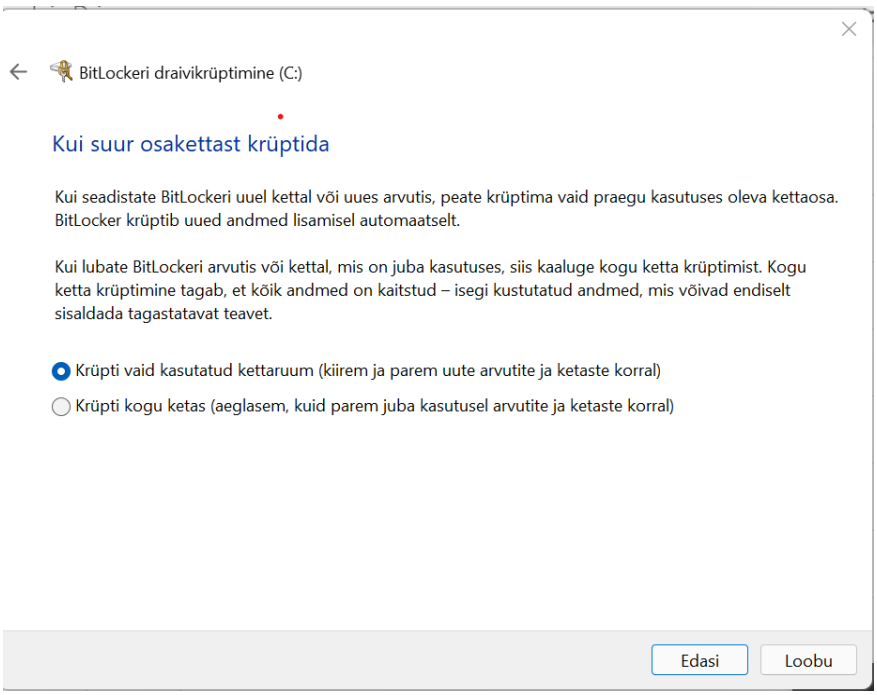


3. Seejärel tuleb BitLocker lihtsalt aktiveerida vajutades „Aktiveeri BitLocker" nupul. Krüteerimine võtab tõepoolest vaid mõned sekundid aega ning avatud dialoogiaken suletakse.

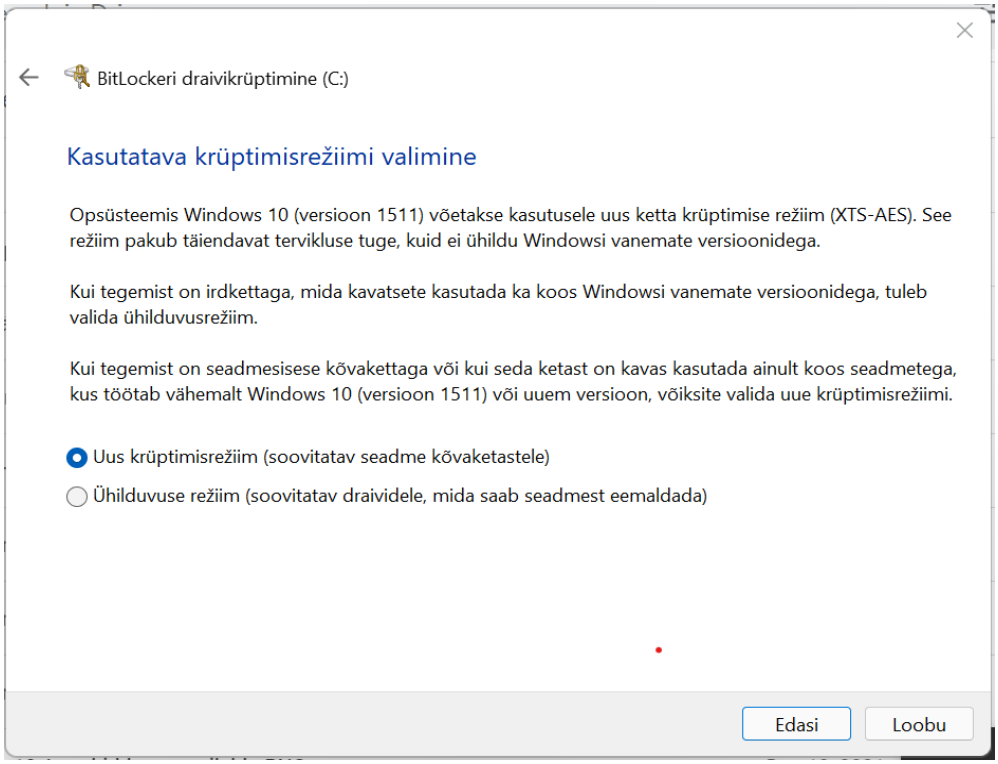


BitLockeri seadistamise protsess kui seadmel on eelseadistus välja lülitatud (või kui varasemalt on BitLocker käsitsi välja lülitatud):

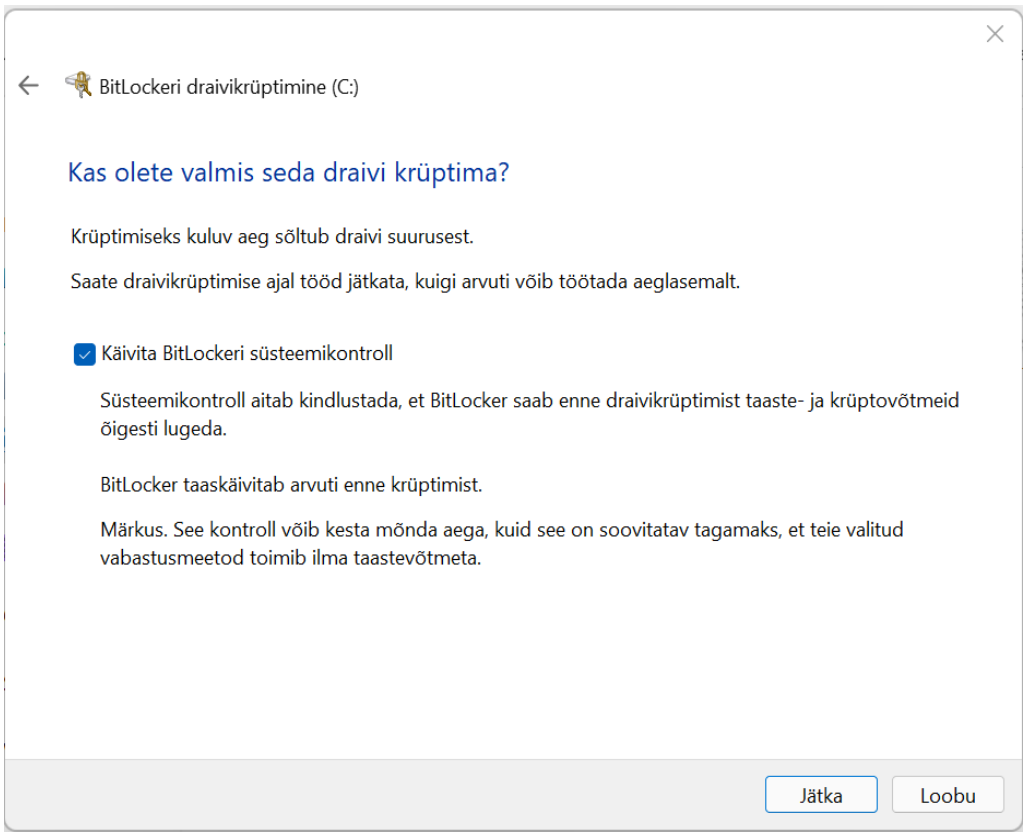
1. Krüpteerimiseks tuleb avada juhtpaneeli alt Süsteem ja turve ning sealt BitLockeri draivikrüptimine. Selles vaates vali "Lülita BitLocker sisse"
2. Järgmiseks tuleb valida kuidas soovite oma taastevõtit varundada. Valikus on kolm varianti: salvestamine Microsofti kontole, salvestamine faili ning taastevõtme printimine.
3. Seejärel tuleb valida kui suur osa kettast krüpteerida, kas osa või kogu ketas.



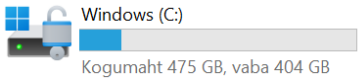
4. Järgmiseks tuleb valida krüptimisrežiim. Uus krüptimisrežiim on XTS-AES algoritmiga.



5. Viimasena tuleb valida kas soovitakse ka süsteemikontrolli. Igas vaates on kõikide seadistuste valikute kohta lisainfo.



Kui ketas on korrektselt seadistatud, siis kuvatakse operatsioonisüsteemi ketast ilma hoiatusikoonita: Seadme registreerimisprotsess Windowsi häälestamisel



Lihtlitsents

Lihtlitsents lõputöö reprodutseerimiseks ja üldsusele kättesaadavaks tegemiseks

Mina, **Keity Raudmäe**,

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) minu loodud teose **„Operatsioonisüsteemi Windowsi 11 standardsed riistvara turbetehnoloogiad ja nende turvaline kasutamine HP Elitebook 840 G8 näitel**“,

   mille juhendaja on **Alo Peets**,

   reprodutseerimiseks eesmärgiga seda säilitada, sealhulgas lisada digitaalarhiivi DSpace kuni autoriõiguse kehtivuse lõppemiseni.

2. Annan Tartu Ülikoolile loa teha punktis 1 nimetatud teos üldsusele kättesaadavaks Tartu Ülikooli veebikeskkonna, sealhulgas digitaalarhiivi DSpace kaudu Creative Commonsi litsentsiga CC BY NC ND 3.0, mis lubab autorile viidates teost reprodutseerida, levitada ja üldsusele suunata ning keelab luua tuletatud teost ja kasutada teost ärieesmärgil, kuni autoriõiguse kehtivuse lõppemiseni.

3. Olen teadlik, et punktides 1 ja 2 nimetatud õigused jäävad alles ka autorile.

4. Kinnitan, et lihtlitsentsi andmisega ei riku ma teiste isikute intellektuaalomandi ega isikuandmete kaitse õigusaktidest tulenevaid õigusi.

Keity Raudmäe

09.03.2022