TAMPEREEN
AMMATTIKORKEAKOULU

BITLOCKER-LEVYNSALAUS

Arkkitehtuuri ja käyttöönotto

Joonas Lakka

Opinnäytetyö
Toukokuu 2017
Tietotekniikan koulutusohjelma
Ohjelmistotekniikka

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietotekniikan koulutusohjelma
Ohjelmistotekniikka

LAKKA JOONAS:
BitLocker-levynsalaus
Arkkitehtuuri ja käyttöönotto

Opinnäytetyö 32 sivua, joista liitteitä 2 sivua
Toukokuu 2017

Tässä opinnäytetyössä perehdyttiin BitLocker-levynsalaustuotteen toimintaan ja sen käyttöönottoon tietoturvallisessa työasemaympäristössä. Työn tuloksia voidaan käyttää esimerkiksi tietoturvallisen BitLocker-konfiguraation muodostamiseen tai eri levynsalaustuotteiden soveltuvuuden arviointiin.

Työssä kuvataan keskeiset BitLocker-levynsalauksen komponentit ja niiden toiminta. Erityisesti huomiota kiinnitetään mekanismeihin, joilla varsinaisen levynsalauksen salausavaimet muodostetaan. Mekanismeista havaittuja ominaisuuksia sovelletaan lopulta käytännön konfigurointimahdollisuuksiin.

BitLocker-levynsalaustuote tarjoaa oletusasetuksillaankin varsin vahvan turvan suojattavalle tiedolle. Korotetun tietoturvan ympäristössä levynsalauksen turvallisuutta voidaan parantaa esimerkiksi vahvemmalla salausavaimella. Korotetun tietoturvan ympäristössä tulee kuitenkin huomioida kaikkien salauksessa käytettyjen avainten vahvuus, sillä salaus on vain niin vahva kuin sen heikoin salausavain.

Asiasanat: windows, bitlocker, levynsalaus, arkkitehtuuri, tietoturva

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree Programme in ICT Engineering
Software engineering

LAKKA JOONAS:
BitLocker disk encryption
Architecture and deployment

Bachelor's thesis 32 pages, appendices 2 pages
May 2017

This thesis examines BitLocker disk encryption product's architecture and deployment possibilities in a security critical environment. The results of this thesis could be used to form a secure BitLocker configuration or to evaluate other existing encryption products.

The thesis aims to describe the principles of the key components of the BitLocker disk encryption product. Particular attention is paid to the way encryption cipher's encryption keys are handled. Identified features of the key architecture are then used to form recommendations for a more secure configuration.

Even with the default configuration the BitLocker disk encryption offers a quite strong protection for user data. To achieve better security, BitLocker can be configured to use stronger encryption key. However, not all key protectors manage to provide the necessary key strength for higher security demands.

Key words: windows, bitlocker, disk encryption, architecture, security

SISÄLLYS

1 JOHDANTO 6
2 LEVYNSALAUS 7
2.1 Käsitteet 7
2.2 BitLocker-levynsalaustuote 8
3 SALAUSALGORITMIT 9
3.1 AES-standardi 9
3.2 Lohkosalauksen ketjutustilat 10
3.2.1 CBC-ketjutustila 11
3.2.2 Elephant diffuser -laajennos 11
3.2.3 XTS-ketjutustila 12
4 SALAUSAVAIMET 13
4.1 Avainhierarkia 13
4.2 Osiokohtaiset avaimet 14
4.3 Käyttäjän määrittämät avaimet 15
4.3.1 TPM-piirin avulla muodostetut avaimet 15
4.3.2 Puhtaat avaimet ja palautusavaimet 17
4.3.3 Palautussalasana 17
5 KONFIGUROINTI 19
5.1 Graafinen käyttöliittymä 19
5.2 Komentorivityökalut 20
5.2.1 Manage-BDE -komentorivityökalu 20
5.2.2 PowerShell-komentotulkki 21
5.3 Ryhmäkäytännöt 22
6 KONFIGURAATION KOVENTAMINEN 24
6.1 Salausmenetelmän valinta 24
6.2 TPM-kirjautumistavan valinta 25
6.3 Palautustapojen valinta 26
7 MUUT LEVYNSALAUSTUOTTEET 27
8 POHDINTA 28
LÄHTEET 29
LIITTEET 31
Liite 1. Esimerkki kovennetusta ryhmäkäytännöstä 31

LYHENTEET JA TERMIT

NIST	National Institute of Standards and Technology, Yhdysvaltojen kansallisen standardi- ja teknologiainstituutti.
AES	Advanced encryption standard, salausalgoritmien standardi.
CBC	Cipher block chaining, lohkosalauksen ketjutustila.
XEX	Xor encrypt xor, lohkosalauksen ketjutustila.
XTS	XEX-based tweaked-codebook mode with ciphertext stealing, XEX-ketjutustilan muunnos.
VMK	Volume master key, BitLockerin salausavaintyyppi.
FVEK	Full volume encryption key, BitLockerin salausavaintyyppi.
RSA	Rivest Shamir Adleman, yleinen julkisen avaimen salausalgoritmi
TPM	Trusted platform module, tietokoneiden salausavainten tallentamiseen tarkoitettu mikroprosessori.
PCR	Platform configuration registers, TPM-piirin ominaisuus tarkistussummien tallentamiseen.

1 JOHDANTO

Käyttäjän data turvataan tietojärjestelmissä erilaisilla käyttöoikeusmäärittelyillä. Datan luvallinen käyttäjä on tyypillisesti määritelty tiedostojärjestelmässä tai erillisessä tietokannassa, josta sen käyttöoikeus varmistetaan käytön aikana esimerkiksi käyttöjärjestelmän tai ohjelmiston toimesta.

Käyttöoikeuden todentaminen tapahtuu kuitenkin vain käyttöoikeusmäärittelyjä tukevia ohjelmistoja käytettäessä. Varsinainen data tallennetaan usein selkokielisenä ja käyttöoikeusmäärittelyt ovat vain datan lisätietoja. Luvaton käyttäjä pystyy siis lukemaan tiedon oikeusmäärittelyistä riippumatta, kunhan pääsee käsiksi tallennusmediaan, esimerkiksi sammutetun työaseman kiintolevyyn.

Tallennetun datan luvaton lukeminen voidaan kuitenkin estää salaamalla tallennukseen käytetty tallennusmedia. Salatun datan lukeminen vaatii ensin salauksen avaamisen, joka onnistuu vain luotetun käyttäjän tai ohjelmiston toimesta. Tällöin voidaan varmistua salauksen avanneen tahon noudattavan tietoon määritettyjä käyttöoikeuksia.

Tässä opinnäytetyössä perehdytään Windows-käyttöjärjestelmissä käytetyn BitLocker-levynsalaustuotteen toimintaan. Työn tarkoitus on arvioida tuotteen teknistä toteutusta ja pohtia miten se vaikuttaa tuotteen tietoturvalliseen käyttöön Windows-työasemien salaamisessa. Erityisesti kiinnitetään huomiota salausavainten käsittelyyn, sillä se vaikuttaa merkittävästi levynsalauksen kokonaistietoturvallisuuteen. Työn tuloksia voidaan käyttää esimerkiksi tietoturvallisen konfiguraation määrittämiseen tai eri levynsalaustuotteiden vertailuun.

2 LEVYNSALAUS

Tässä luvussa esitellään yleisesti levynsalaukseen liittyviä käsitteitä ja BitLocker-levynsalaustuotteen ominaisuudet.

2.1 Käsitteet

Levynsalaus

Levynsalauksella (disk encryption) suojataan tietokoneen kiintolevy, muu tallennusmedia tai niiden osio luvattomalta käytöltä tietokoneen ollessa sammutettuna. Levynsalaus toteutetaan tyypillisesti ohjelmistolla tai ajurilla joka tulkkaa käyttöjärjestelmän tekemät luku- ja kirjoitusoperaatiot määrätyllä salausalgoritmilla ja salausavaimella. Tällöin levylle tallennetaan aina vain algoritmilla sekoitettua dataa, eikä sen sisältöä voida tulkita käytettyä algoritmia ja salausavainta tietämättä. (TechNet 2009.)

Salausalgoritmi ja salausavain

Salausalgoritmi kuvaa ne operaatiot, joilla varsinainen data salataan. Salausalgoritmi ottaa syötteenä salattavan datan sekä yksilöivän salausavaimen ja antaa tuloksena salatun datan. Levynsalauksessa käytetään usein symmetrisen avaimen salausta (symmetric-key encryption), jolloin salausalgoritmi käyttää samaa avainta datan salaamiseen ja salauksen purkamiseen. (Delfs, Knebl 2015, 11-12.)

Koskemattomuus

Järjestelmän koskemattomuuden varmistamisella pyritään tunnistamaan salattuun dataan ja käyttöjärjestelmän tietoturvaan kohdistuvia uhkia. Levynsalaus itsessään on tapa varmistaa salatun tiedon koskemattomuus. Vaikka käyttöjärjestelmän järjestelmäosio olisi salattu, tulee sen salaus avata käynnistyksen aikana salaamattomalla käynnistysosiolla. Salaamaton osio onkin altis erilaisille tiedonkalasteluhyökkäyksille. Tyypillisesti käynnistysosion koskemattomuus ja eheys varmistetaan vertailemalla sen tarkistussummia ohjelmallisin keinoin, mahdollisesti erillisellä laitteistolla tuettuna. (TechNet 2009.)

2.2 BitLocker-levynsalaustuote

BitLocker on Microsoftin kehittämä levynsalaustuote, joka sisältyy valittuihin Windows-käyttöjärjestelmän versioihin (taulukko 1). BitLockerin tärkeimmät tehtävät ovat kiintolevyllä olevan tiedon suojaaminen sekä järjestelmän koskemattomuuden varmistaminen. Se on osa Windows-käyttöjärjestelmää, eikä sitä tarvitse erikseen asentaa. (BitLocker Drive Encryption Step-by-Step Guide 2009.)

Taulukko 1: BitLockerin tuetut käyttöjärjestelmät

Käyttöjärjestelmä	**Versio**
Windows Vista	Enterprise, Ultimate
Windows 7	Enterprise, Ultimate
Windows 8 ja 8.1	Enterprise, Professional
Windows 10	Enterprise, Professional, Education
Windows Server 2008 ja uudemmat	Kaikki versiot

Varsinaiseen levynsalaukseen BitLocker käyttää AES-standardin mukaista salausalgoritmia, joko 128- tai 256-bittisellä salausavaimella. Salausalgoritmin tukena käytetään Windows-versiosta riippuen joko CBC- tai XTS-ketjutustilaa. Salausavainten arkkitehtuuri perustuu paikallisesti generoitavaan sisäkkäisten avainten hierarkiaan. Järjestelmän koskemattomuuden varmistaminen tapahtuu käytännössä järjestelmän käynnistysosion eheyden varmistamisella. Käynnistysosion eheys varmistetaan yhteensopivan TPM-turvapiirin avulla. (Bitlocker: AES-XTS 2016; BitLocker Drive Encryption Step-by-Step Guide 2009.)

BitLockeria on mahdollista käyttää niin henkilökohtaisella työasemalla kuin yrityksen hallitussa ympäristössä. BitLockerin saa oletusasetuksilla käyttöön suoraan Windowsin käyttöliittymästä, eikä sen konfigurointi vaadi erityistä teknistä tuntemusta. Vaikka kaikkia tuotteen ominaisuuksia ei voi konfiguroida suoraan käyttöliittymästä, tarjoaa se samat ominaisuuden niin henkilökohtaisille tietokoneille kuin yrityksen hallituille työasemille. (BitLocker Drive Encryption Step-by-Step Guide 2009.)

3 SALAUSALGORITMIT

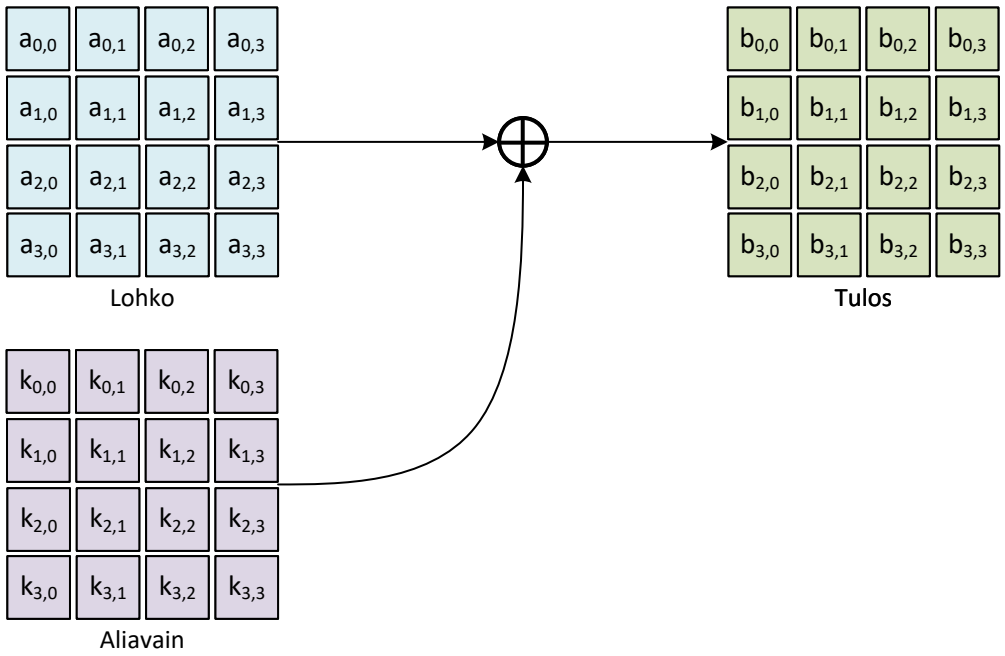
Tässä luvussa esitellään BitLockerin käyttämä AES-salausalgoritmi ja sen kanssa käytetyt ketjutustilat. Luvun tarkoitus on antaa lukijalle yleiskäsitys käytetyn algoritmin toimintaperiaatteista sekä algoritmeihin liittyvistä käsitteistä. Algoritmien perusteiden avaaminen mahdollistaa BitLockerin ominaisuuksien vertaamisen muihin tuotteisiin ja auttaa ymmärtämään seuraavan luvun avainhierarkian käsittelyä. Opinnäytetyön toteuttaminen ei kuitenkaan vaadi salausalgoritmien teorian syvällistä ymmärtämistä.

3.1 AES-standardi

Advanced encryption standard (AES) on Yhdysvaltojen kansallisen standardi- ja teknologiainstituutin (NIST) määrittelemä salausalgoritmien standardi. AES-standardissa käytetään Rijndael-lohkosalausalgoritmia sen 128-bittisellä lohkokoolla sekä 128-, 192- ja 256-bittisellä avainpituudella. Varsinainen Rijndael-algoritmi tukee myös useita muita lohko- ja avainkokoja. (Delfs, Knebl 2015, 19; National Institute of Standards and Technology 2011.)

BitLocker käyttää AES-algoritmia joko 128- tai 256-bittisellä avainkoolla. Käytetty avainkoko ilmenee käyttöliittymässä salaustavan nimeämisestä. Esimerkiksi AES 128-bit tarkoittaa algoritmin 128-bittistä avaimenpituutta. (BitLocker™ Drive Encryption Security Policy 2011, 13)

Rijndael-lohkosalausalgoritmissa data salataan määrätyn mittaisina bittijonoina, eli ns. lohkoina. Lohkoja käsitellään tavuista koostuvina matriiseina, joille iteroidaan erilaisia solu-, rivi- ja sarakeoperaatioita. Jokaista algoritmin iteraatiota kutsutaan kierrokseksi (round). Kierroksen aikana lohkolle tehdään muun muassa sarakekohtaisia kertolaskuja, rivinsiirto-operaatioita sekä loogisia XOR-operaatioita salausavaimen osien kanssa. Kuviossa 1 esitetään Rijndael-algoritmin AddRoundKey-vaihe, jossa avaimen osa *k* liitetään salattavan lohkon sen hetkiseen tilaan *a* loogisella XOR-operaatiolla. (Delfs, Knebl 2015, 19-25.)



Kuvio 1: Rijndael-algoritmin AddRoundKey -vaihe.

3.2 Lohkosalauksen ketjutustilat

Lohkosalausalgoritmit, kuten AES, salaavat tiedon kokonaisina lohkoina. Kun salattavan tiedon koko on suurempi kuin käytetyn algoritmin lohkokoko, käytetään varsinaisen algoritmin tukena erilaisia ketjutustiloja (block cipher mode of operation). Ketjutustila määrittelee ne operaatiot, joilla varsinaista salausalgoritmia toistetaan lohkokokoa suurempien datamäärien kanssa. (Delfs, Knebl 2015, 25-26.)

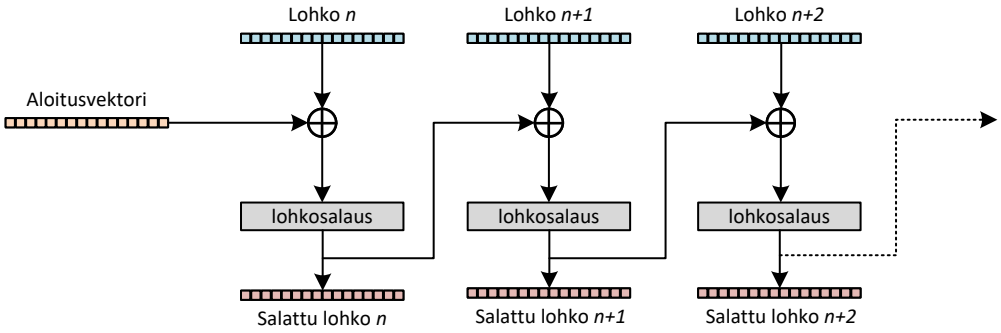
Ketjutustilan avulla peräkkäiset salatut lohkot saadaan riippuvaisiksi toisistaan. Ideaalisessa tilanteessa suurempi tietomassa muuttuu lohkosalauksen ketjutuksen ansiosta pseudosatunnaiseksi, eikä identtisiä salattuna tallennettuja lohkoja pysty suoraan tunnistamaan. Ketjutuksella siis vaikeutetaan salattujen lohkojen muuttamista ja salausavaimen arvaamista tunnettujen identtisten lohkojen avulla. (Delfs, Knebl 2015, 25-26.)

BitLocker käyttää oletuksena CBC-ketjutustilaa. Uusien Windows-versioiden myötä BitLockeriin on kuitenkin lisätty tuki myös Elephant diffuser -laajennokselle sekä XTS-ketjutustilalle. Uudet ketjutustilat ilmaistaan käyttöliittymässä salaustavan nimeämisen lisäosalla. Esimerkiksi XTS-AES taas tarkoittaa, että käytössä on CBC-ketjutustilan sijaan XTS-ketjutustila. Jos ketjutustilaa ei ole erikseen ilmoitettu, käytetään CBC-ketjutustilaa. (BitLocker: AES-XTS 2016)

3.2.1 CBC-ketjutustila

CBC, eli cipher block chaining, on yleinen lohkosalauksen ketjutustila, jota on käytetty myös esimerkiksi DES-salausalgoritmin kanssa. Se on esimerkiksi Yhdysvaltojen standardi- ja teknologiainstituutin (NIST) hyväksymä ketjutustila tiedon luottamuksellisuuden varmistamiseen. CBC-ketjutustila on tuettuna kaikissa Windows-versioissa. (Block cipher modes 2016.)

CBC-ketjutustilassa jokaiseen salaamattomaan lohkoon yhdistetään loogisella XOR-operaatiolla edellisen lohkon salattu tulos (Kuvio 2). Sarjan ensimmäinen lohko alustetaan erillisellä alustusvektorilla, joka voidaan määritellä varsinaisen salausavaimen tavoin satunnaisesti generoituna. Levynsalauksessa CBC-ketjutustila alustetaan tyypillisesti uudelleen jokaiselle kiintolevyn sektorille, sillä muuten jokainen muutos vaatisi myös kaikkien sen jälkeisten lohkojen uudelleensalauksen. (Delfs, Knebl 2015, 26-27.)



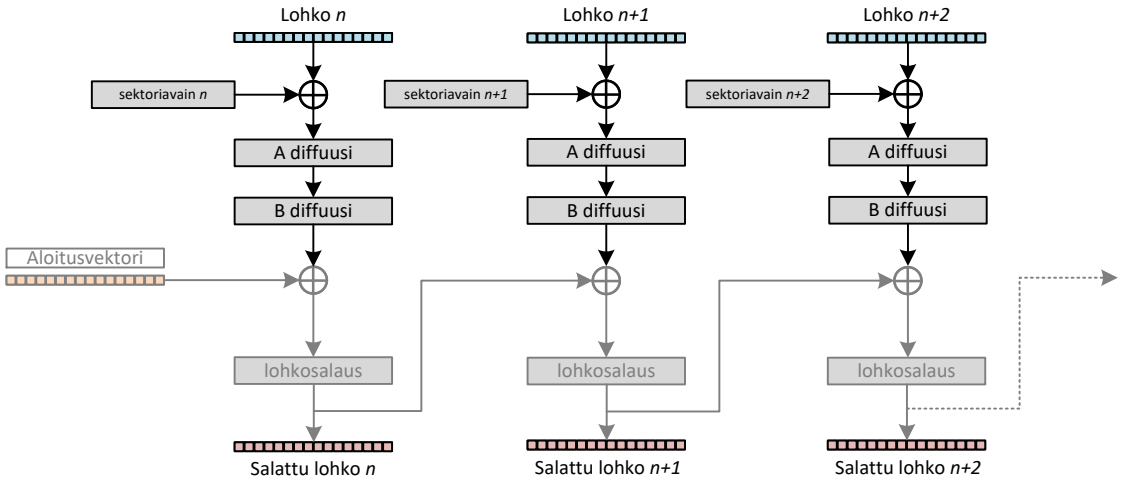
Kuvio 2: Lohkosalauksen CBC-ketjutustila.

3.2.2 Elephant diffuser -laajennos

Elephant diffuser on Microsoftin itse kehittämä CBC-ketjutustilan laajennos. Elephant diffuserin tarkoitus oli parantaa vanhan CBC-ketjutustilan turvaa erinäisiä datan manipulointihyökkäyksiä kohtaan. Vaikka Elephant diffuser tarjoaa teoriassa paremman tietoturvan, ei sillä kuitenkaan ole NIST:n sertifiointia. (Microsoft Corporation 2006; Kornblum 2009, 2.)

Elephant diffuser julkaistiin Windows 7 -käyttöjärjestelmän mukana. Sen tuki kuitenkin lopetettiin jo Windows 8:n julkaisussa suorituskykytekijöihin vedoten.

Elephant diffuserissa jokainen salattavaan lohko liitetään loogisella XOR-operaatiolla sektorikohtaiseen avaimeen, ja tulokselle tehdään kaksi diffuusio-operaatiota (Kuvio 3). Diffuusio-operaatioissa jokainen salattava lohko sidotaan myös sektorin muiden lohkojen sisältöön. Tällöin pienikin muutos salattavassa lohkossa aiheuttaisi mahdollisimman suuren muutoksen koko sektorissa. Microsoftin diffuusiosovelluksen jälkeen lohko käsitellään kuten CBC-ketjutustilassa, käsitelty lohko liitetään edellisen lohkon salattuun tulokseen ja salataan. (Microsoft Corporation 2006; Kornblum 2009.)



Kuvio 3: Lohkosalauksen CBC-ketjutustila Elephant diffuserilla

3.2.3 XTS-ketjutustila

XTS-ketjutustila on yleisesti käytetyn XEX-ketjutustilan muunnos. XEX-ketjutustilan (xor-encrypt-xor) perusidea on, että kulloinkin käsiteltävä lohko yhdistetään sarakekohtaiseen komponenttiin sekä ennen varsinaista lohkosalausta, että sen jälkeen. XTS-ketjutustilassa tähän on lisätty niin sanottu ciphertext stealing -ominaisuus, joka mahdollistaa vajaan lohkon yhdistämisen toiseksi viimeisen lohkon kanssa. (Block cipher modes 2016.)

IEEE on virallisesti standardoinut XTS-ketjutustilan käytön AES:n kanssa osana IEEE P1619 -standardia. Myös Yhdysvaltojen NIST on hyväksynyt IEEE-standardin mukaisen XTS-ketjutustilan käytön tiedon luottamuksellisuuden varmistamiseen. XTS-ketjutustilan tuki esiteltiin Windows 10:n November Updaten yhteydessä (1511). (Block cipher modes 2016.)

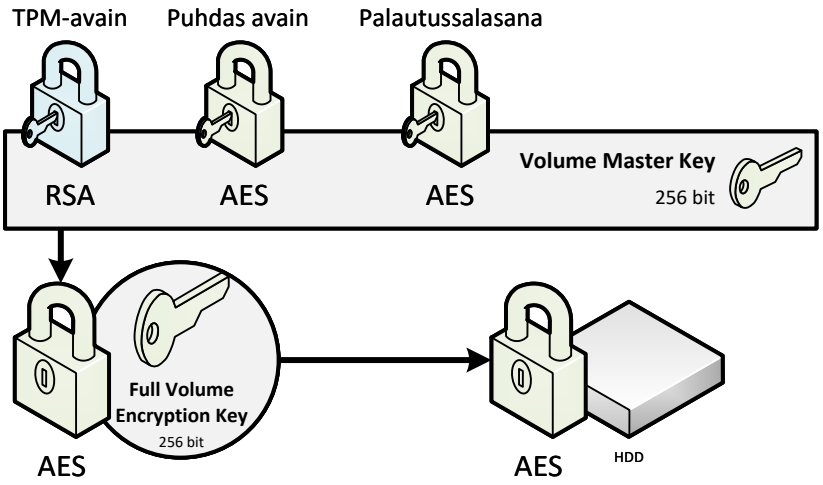
4 SALAUSAVAIMET

Tässä luvussa esitellään BitLockerin salausavainarkkitehtuuri sekä sen keskeiset osat ja käsitteet. Erityisesti pureudutaan mekanismeihin, joilla käyttäjän syötteestä muodostetaan varsinainen salausalgoritmin käyttämä salausavain. Salausavainten käsittely on merkittävä osa levynsalaustuotteen turvallisuutta ja sen toimintaperiaatteiden ymmärtäminen on tietoturvallisen konfiguraation muodostamiseksi elintärkeää.

4.1 Avainhierarkia

Salausavaimen vaihtaminen muuttaa aina salatun datan tulkintaa, joten kaikki tietyllä avaimella salattu data pitää avaimen muutoksen jälkeen salata uudelleen. Muiden salaustuotteiden tapaan BitLockerin avainarkkitehtuuri perustuukin sisäkkäiseen avainhierarkiaan. Varsinainen kiintolevyn salaukseen käytetyt avaimet on tallennettu salattuna osion yhteyteen, eikä niihin tehdä käytön aikana muutoksia. Käyttäjällä taas voi olla useita toisistaan eroavia salausavaimia, joilla varsinainen salausavain saadaan lopulta avattua. (Microsoft 2007; Delfs, Knebl 2015, 11-12)

BitLockerissa varsinainen data on salattu FVEK-avaimella, eli full volume encryption key:llä. FVEK-avain taas salataan VMK-avaimella, eli volume master key:llä. VMK-avain salataan lopulta jokaisella käyttäjän salausavaimella erikseen (Kuvio 4). Sama VMK-avain tallennetaan siis itseasiassa useaan kertaan. Käyttäjän määrittämät salausavaimet voidaan johtaa esimerkiksi laitteistoavusteisesti TPM-turvapiirillä tai suoraan käyttäjän syöttämästä palautussalasanasta. (BitLocker™ Drive Encryption Security Policy 2011, 9.)

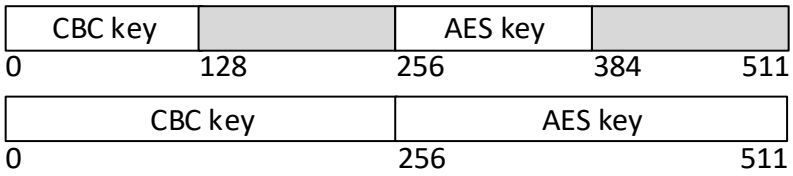


Kuvio 4: BitLocker avainhierarkia.

4.2 Osiokohtaiset avaimet

Sekä VMK- että FVEK-avain muodostetaan automaattisesti kullekin salatulle osiolle. Avaimet tallennetaan aina salatun osion yhteyteen. Avaimia voi muuttaa vain purkamalla koko salaus ja käynnistämällä se uudelleen. (Microsoft 2011, 9.; Kornblum 2009, 2.)

FVEK-avainta käytetään varsinaisen datan salaamiseen. FVEK-avain sisältää joko 128- tai 256-bittisen AES-osan sekä yhtä suuren ketjutustilan osan. FVEK-avain on käytetystä avainpituudesta riippumatta aina 512-bittinen, mutta ylimääräinen osa on 128-bittisellä avaimella käyttämättä (Kuvio 5). FVEK-avaimen salaamiseen käytetty VMK-avain on valitusta avaimenpituudesta riippumatta aina 256-bittinen. (J. Kornblum 2009, 2.)



Kuvio 5: FVEK-avaimen rakenne.

4.3 Käyttäjän määrittämät avaimet

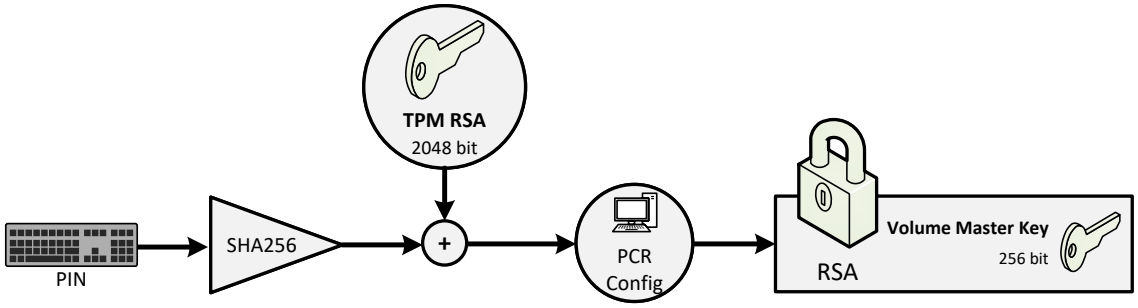
Automaattisesti muodostetut avaimet, kuten FVEK- ja VMK-avaimet, generoidaan satunnaislukufunktioilla aina suoraan oikean kokoisiksi. Käyttäjän syötteestä ei kuitenkaan yleensä saada täsmälleen toivotun avainpituuden mukaista avainta. Käyttäjän määrittämissä avaimissa varsinainen salausavain muodostetaankin syötteen ja erilaisten väliavainten sekä tarkistussummien yhdistelmistä. Tässä luvussa esitellään keskeiset käyttäjän määriteltävissä olevat salausavaintyypit ja niiden muodostamismenetelmät.

4.3.1 TPM-piirin avulla muodostetut avaimet

TPM-piiri, eli trusted plattform module, on tietokoneiden kryptografiseen suojaukseen dedikoitu mikrokontrolleri. TPM-piiriä käytetään tyypillisesti työaseman salaukseen käytettyjen avainten sekä käyttöjärjestelmän eheyden varmistamiseen käytettyjen tarkistussummien turvalliseen tallentamiseen. TPM-piiri integroidaan nykyään lähes kaikkien uusien työasemien emolevylle. (Trusted Platform Module Technology Overview 2017.)

TPM-piirin toiminta levynsalauksessa perustuu 2048-bittisen RSA-avaimen käyttöön VMK-avaimen salauksessa. AES-algoritmista poiketen RSA perustuu julkisen avaimen salaukseen. Kun käyttöjärjestelmä alustaa TPM-piirin käyttöönsä, muodostuu yksityisen ja julkisen avaimen pari. Yksityinen avain jää vain TPM-piirin tietoon ja varsinainen tieto salataan julkisella avaimella. Julkisella avaimella salattu tieto taas voidaan avata vain vastaavalla yksityisellä avaimella. TPM-piirillä salatun avaimen avaaminen onnistuu siis vain sillä TPM-piirillä, jolla salaus on alkujaan tehty. (BitLocker™ Drive Encryption Security Policy 2011, 8; Delfs, Knebl 2015, 49.)

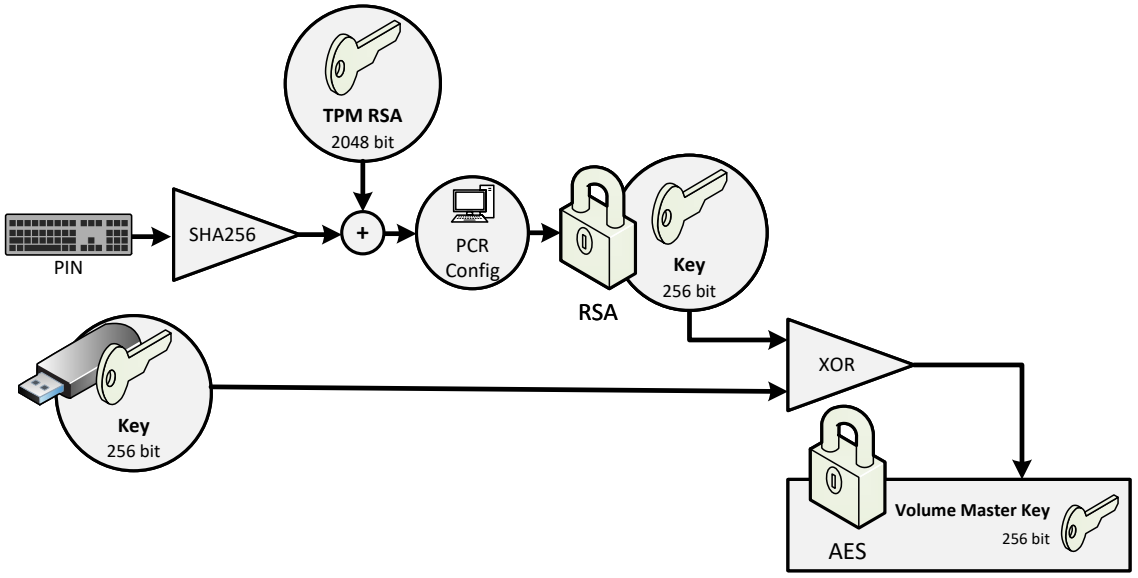
Kun VMK-avain suojataan pelkällä TPM-piirillä tai TPM-piirillä sekä PIN-koodilla, sen salaus tapahtuu suoraan TPM-piirin RSA-avaimella (Kuvio 6). Mahdollisesta PIN-koodista muodostetaan SHA256-tarkistussumma, joka yhdistetään TPM-piirin avaimeen. Ennen varsinaisen VMK-avaimen avaamista käynnistysosion koskemattomuus varmistetaan TPM-piirin PCR Config -toiminnon avulla. (BitLocker™ Drive Encryption Security Policy 2011, 8.)



Kuvio 6: VMK-avaimen avaaminen TPM-piirin ja PIN-koodin avulla.

TPM-piirin kanssa käytetty PIN-koodi voi olla maksimissaan 20 merkkiä pitkä. PIN-koodi voi oletuksena pitää sisällään vain numeroita, mutta lisäasetuksilla siinä voidaan sallia myös US-näppäimistöasettelun mukaiset kirjaimet ja merkit. PIN-koodille ei kuitenkaan voi pakottaa minkäänlaista kompleksisuusvaatimusta.

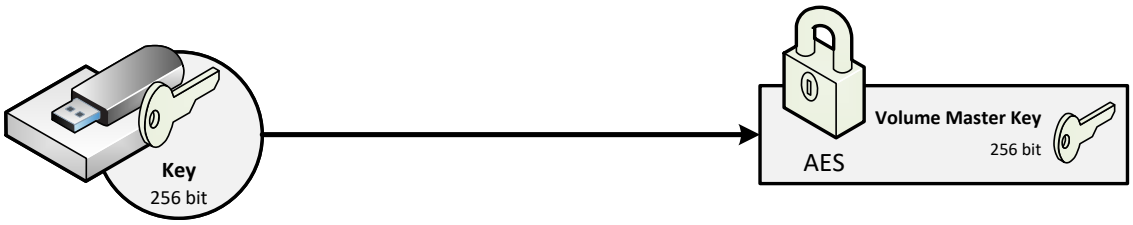
Jos VMK-avaimen suojaukseen käytetään TPM-piirin lisäksi niin sanottua käynnistysavainta, avausprosessiin joudutaan lisäämään väliavain (Kuvio 7). TPM-piiriä käytetäänkin tällöin 256-bittisen väliavaimen salaamiseen. Varsinaisen VMK-avaimen salaus saadaan avattua, kun TPM-piirillä avattu väliavain liitetään ulkoiseen käynnistysavaimeen loogisella XOR-operaatiolla. (BitLocker™ Drive Encryption Security Policy 2011, 8.)



Kuvio 7: VMK-avaimen avaaminen TPM-piirin ja käynnistysavaimen kanssa.

4.3.2 Puhtaat avaimet ja palautusavaimet

Puhdas avain (clear key) ja palautusavain (recovery key) ovat satunnaisesti muodostettuja 256-bittisiä avaimia joilla voi suoraan avata VMK-avaimen. Puhdas avain muodostetaan satunnaisesti, eikä käyttäjä voi vaikuttaa sen muotoon. Puhtaita avaimia käytetään sellaisenaan joko salattujen järjestelmäosioiden tai erillisten datalevyjen avaamiseen (Kuvio 8). (BitLocker™ Drive Encryption Security Policy 2011, 8.)



Kuvio 8: VMK-avaimen avaaminen puhtaalla avaimella.

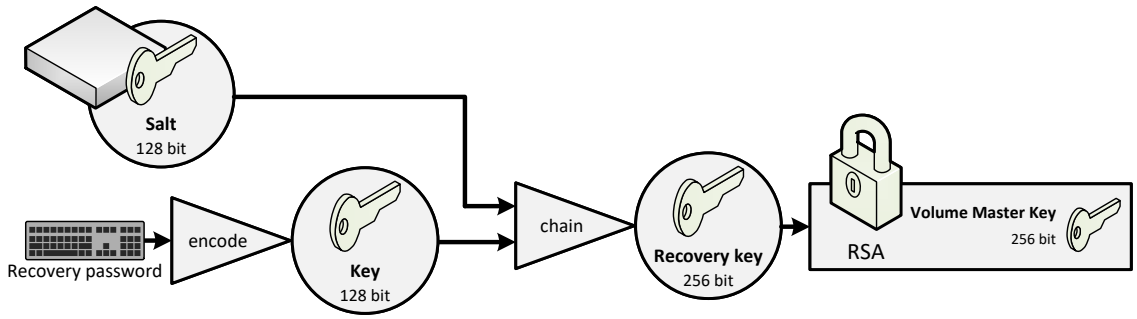
Kaikki käynnistysavaimet eivät kuitenkaan ole puhtaita avaimia. TPM-piirin kanssa käytettävä käynnistysavain on teknisesti ottaen kuten puhdas avain, mutta sillä ei pysty suoraan avaamaan salattua VMK-avainta. (BitLocker™ Drive Encryption Security Policy 2011, 8.)

4.3.3 Palautussalasana

Palautussalasana on BitLockerin oletusarvoinen palautumistapa muiden suojaustapojen ongelmatilanteissa. Se on 48 merkkinen numeerinen salasana joka generoidaan automaattisesti salauksen käynnistämisen yhteydessä. Palautussalasana muodostetaan satunnaisesti, eikä käyttäjä pysty vaikuttamaan sen muotoiluun. (Keys to Protecting Data with BitLocker Drive Encryption 2007.)

Salasana koostuu kahdeksasta kuuden numeron ryhmästä. Palautussalasanan generointifunktio luo 128-bittisen avaimen, joka jaetaan kahdeksaan 16 bitin osaan kunkin numeroryhmän luomiseksi. Jokaisen ryhmän viisi ensimmäistä numeroa kuvastavat varsinaista salasanaa ja kuudes numero on näiden tarkistussumma. Kirjoitusvirheiden havaitsemiseksi salasanan syöttövaiheessa on jokainen numeroryhmä jaollinen luvulla 11. (Kornblum. 2009.)

VMK-avainta avattaessa syötetty 128-bittinen salasana yhdistetään 128-bittiseen kiintolevylle tallennettuun suolaan 256-bittisen avaimen muodostamiseksi (Kuvio 9). Koska salatun osion yhteyteen tallennettu suola on myös hyökkääjän nähtävillä, jää avaimen entropia tietoturvan kannalta siis vain 128-bittiseksi.



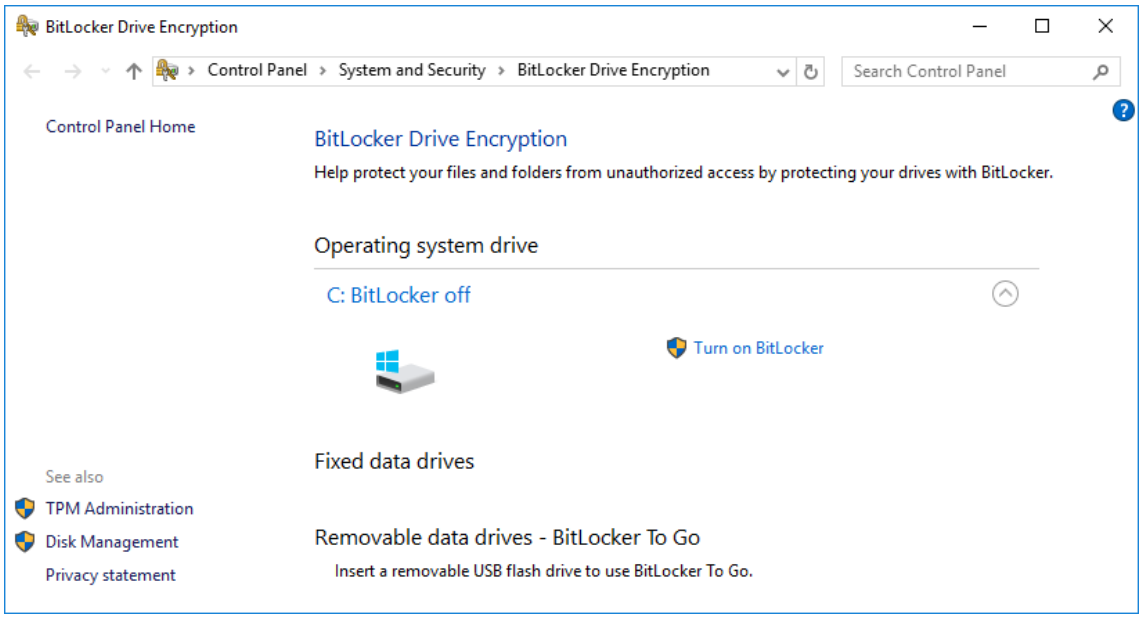
Kuvio 9: VMK-avaimen avaaminen palautussalasanalla.

5 KONFIGUROINTI

Tässä luvussa esitellään keskeisiä BitLockerin konfiguroimiseen ja hallintaan tarkoitettuja työkaluja ja niiden toimintaperiaatteita. Luku tarjoaa perustiedot edellä käsiteltyjen algoritmien ja avainten konfiguroimiseen käytännössä. Konfiguraation perusymmärrys auttaa myös arvioimaan erilaisia tuotteen tietoturvaan kohdistuvia uhkakuvia.

5.1 Graafinen käyttöliittymä

BitLockerin käyttöliittymä on integroitu osaksi Windowsia. Tallennusmedioihin liittyvät keskeiset toiminnot on lisätty hakemistoselaimen kontekstivalikkoihin, ja muut käyttäjän määriteltävissä olevat asetukset on koottu Ohjauspaneeliin omalle sivulleen (Kuva 1).



Kuva 1: Ohjauspaneelin käyttöliittymä.

Käyttöliittymä mahdollistaa vain yksinkertaiset toimenpiteet, kuten salauksen alustamisen oletusasetuksilla, salauksen keskeyttämisen sekä salauksen purkamisen. Käyttäjä voi määrittää esimerkiksi salauksen PIN-koodin ja palautusavaimen tallennuspaikan, mutta esimerkiksi käytettyä salaustapaa tai salauksen avausmenetelmiä ei voi muuttaa. Tarkempien asetusten määrittäminen vaatii joko komentorivityökalujen käyttämistä tai ryhmäkäytäntöjen (group policy) määrittämisen. (BitLocker Drive Encryption Step-by-Step Guide 2011.)

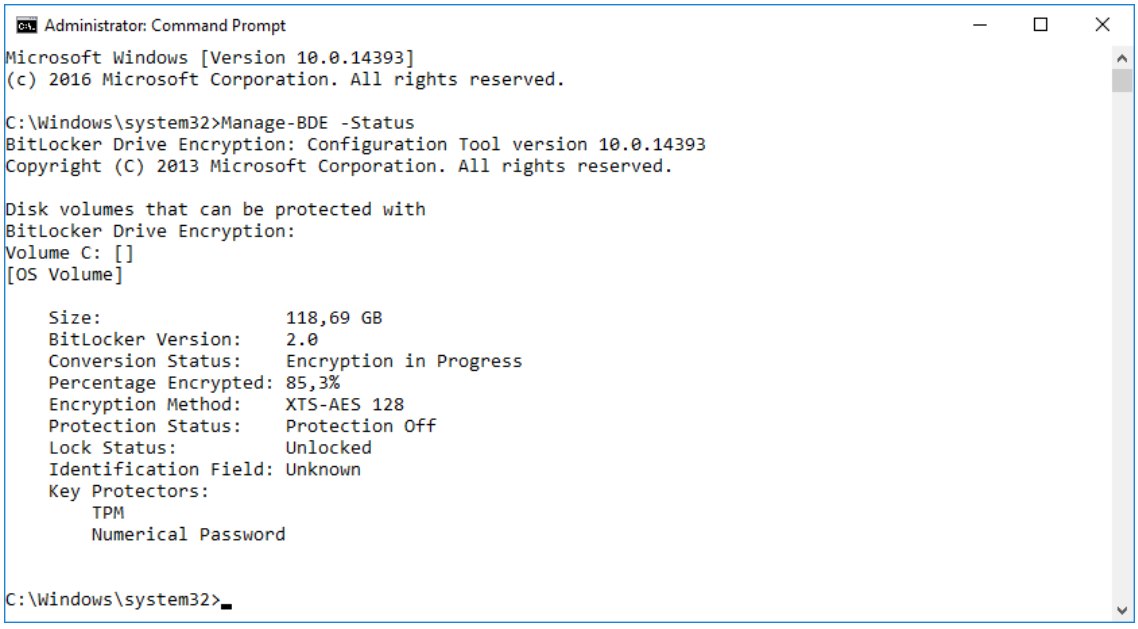
5.2 Komentorivityökalut

BitLockerin edistyksellisempi käskyttäminen onnistuu sen komentorivityökaluja käyttäen. Komentorivityökalut mahdollistavat paikallisen BitLocker-levynsalauksen kaikkien ominaisuuksien konfiguroimisen ja suoran käskyttämisen. Keskeiset BitLockerin konfiguroimiseen tarvittavat toiminnot yhdistettiin alkujaan Manage-BDE -nimiseen komentorivityökaluun. Sittemmin työkalun ominaisuuksia on kuitenkin ryhdytty siirtämään uusiin PowerShell -komentoihin.

5.2.1 Manage-BDE -komentorivityökalu

Windowsin perinteiselle komentokehotteelle tarkoitettua työkalua käytetään syöttämällä sille parametreina haluttu toimenpide ja toimenpiteen vaatimat lisätiedot. Samalla työkalulla voidaan muun muassa lukea salattujen osioiden tietoja, alustaa uusia salattuja osioita, alustaa työaseman TPM-piiri, lisätä tai poistaa salatun osion suojaustapoja sekä purkaa osion salaus. (Manage-bde 2013)

Oletusasetuksilla salatun järjestelmäosion tiedot voitaisiin työkalulla lukea Kuva 2 mukaisesti. Komennon tulosteesta käy ilmi muun muassa salatun osion tiedot, käytetty salausalgoritmi (encryption method), lukituksen avaus (lock status) sekä käytetyt suojaustavat (key protectors).

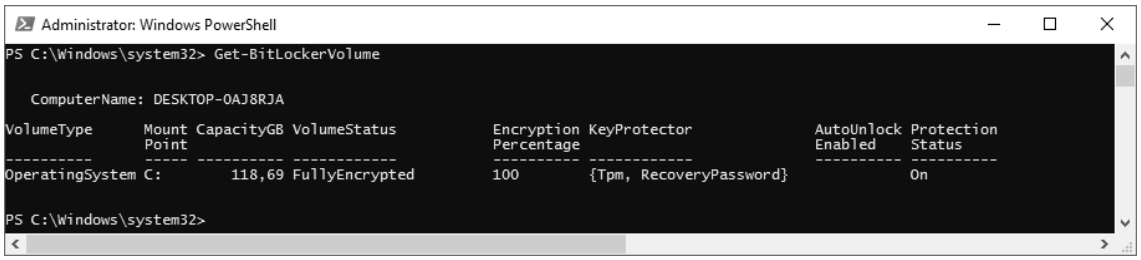


Kuva 2: Manage-BDE-työkalun status-tuloste.

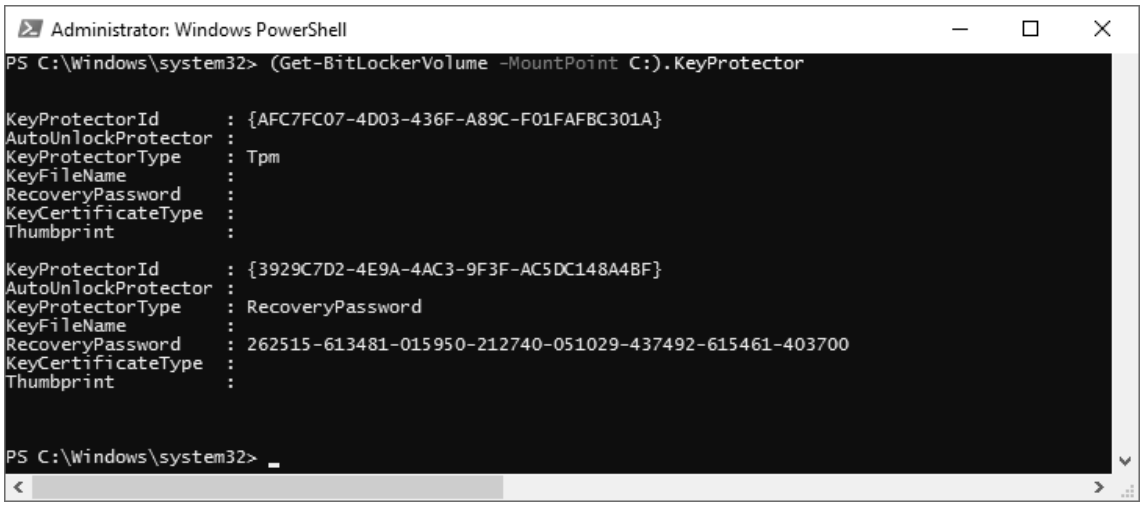
5.2.2 PowerShell-komentotulkki

PowerShell on Microsoftin kehittämä .NET -kirjastoihin perustuva oliokeskeinen komentotulkki. PowerShellissä voidaan perinteisten komentoriviohjelmien lisäksi ajaa niin sanottuja cmdlet-komentoja, jotka palauttavat ajon tuloksen jonkinlaisessa tietorakenteessa. Esimerkiksi työhakemiston sisällön hakeva Get-ChildItem -komento palauttaa tekstimuotoisen tulosteen sijaan listan jokaisesta alikansion ja tiedoston PowerShell-oliosta. PowerShellin cmdlet-komennot nimetään tyypillisesti operaatiota kuvaavalla verbillä ja toimintoa kuvaavalla substantiivilla. (Scripting with Windows PowerShell 2014.)

Manage-BDE -komennon status-esimerkkiä vastaava komento on PowerShellissä Get-BitLockerVolume (Kuva 3). PowerShell-komento palauttaa tietorakenteen, josta komentotulkki pyrkii muodostamaan parhaan visuaalisen esityksen. Komentotulkin esitys ei välttämättä näytä kaikkia palautetun tietorakenteen kenttiä, ja esimerkiksi suojaustavat (KeyProtectors) on esitetty vain palautettujen olioiden nimillä. Käytetyt suojaustavat saakin tulostettua näppärästi viittaamalla kuvan 4 tavoin PowerShell-komentokehotteessa suoraan niiden olioon. (BitLocker Cmdlets in Windows PowerShell 2012.)



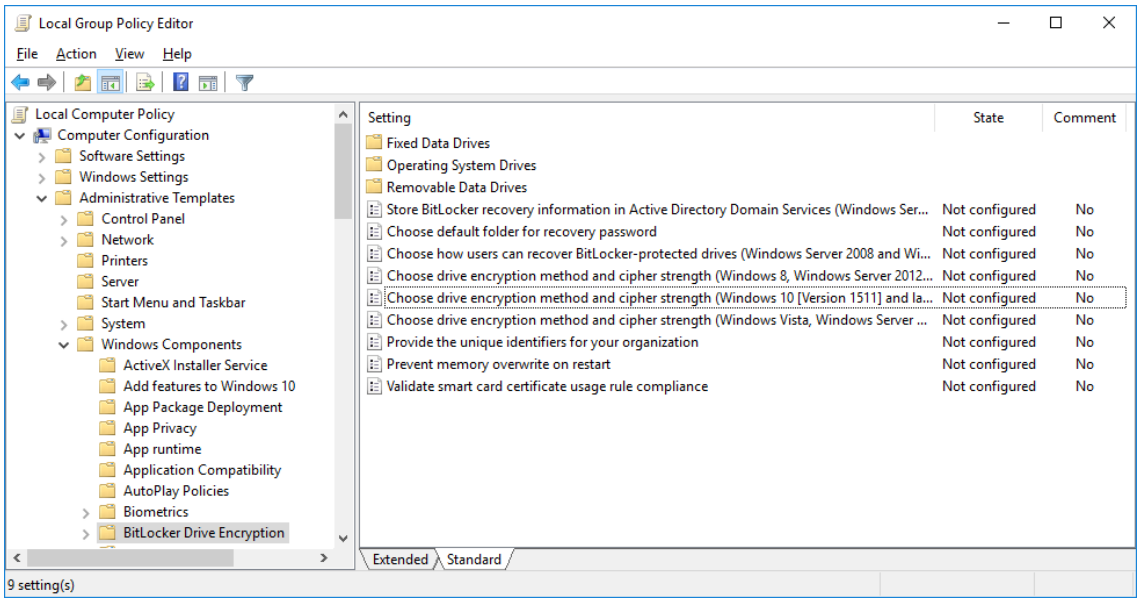
Kuva 3: Get-BitLockerVolume -komennon tuloste.



Kuva 4: Get-BitLockerVolume -komennon suojaustapojen tarkempi listaus.

5.3 Ryhmäkäytännöt

Ryhmäkäytännöt (group policy) on Windows-käyttöjärjestelmien ominaisuus, jolla voidaan konfiguroida useita käyttöjärjestelmän toimintaan liittyviä asetuksia. Yleensä ryhmäkäytännöillä hallitaan Active Directory -toimialueeseen (domain) kuuluvia työasemia. Toimialueessa ryhmäkäytännöt määritellään eri organisaatioyksikköihin (organizational unit) tai käyttöoikeusryhmiin (security group) kohdistettavilla ryhmäkäytäntöobjekteilla (group policy object). Ryhmäkäytäntö voidaan kuitenkin määrittää toimialueesta riippumatta myös paikallisella ryhmäkäytäntöeditorilla (local group policy editor) (Kuva 5). (Group Policy for Beginners 2011.)



Kuva 5: Paikallinen ryhmäkäytäntöeditori.

Ryhmäkäytännöillä käyttöjärjestelmä voidaan pakottaa käyttämään BitLocker-levynsalausta vain määrätyillä asetuksilla. Ryhmäkäytännöllä voidaan esimerkiksi kieltää ei-toivotun palautusavaintyypin käyttö tai pakottaa tietyn avainpituuden käyttö. Jos asetus on määritelty ryhmäkäytännöllä, ei sitä voi muuttaa käyttöliittymässä tai komentorivityökaluilla. Ryhmäkäytännöillä ei kuitenkaan suoraan voi käskyttää kohdetyöaseman BitLocker-levynsalausta. Asetusten määrittelyn jälkeen salauksen käyttöönotto, purkaminen ja muut toimenpiteet tulee tehdä siihen tarkoitetuilla työkaluilla, esimerkiksi käyttöliittymässä tai komentorivityökaluilla.

Esimerkki ryhmäkäytännön asetuksista

Ryhmäkäytännöt tarjoavat useita erillisiä asetuksia BitLockerin hallintaan. Opinnäytetyössä muodostettiin esimerkiksi Windows 10 -työaseman paikallinen ryhmäkäytäntö, jossa määriteltiin perusasetukset työssä käsiteltyjen ominaisuuksien määrittämiseksi (liite 1). Koska eri asetukset on eritelty useisiin asetuksiin ja osin käyttöjärjestelmäkohtaisesti, kannattaa ryhmäkäytäntöjen määrittämisessä turvautua aina Microsoftin dokumentaatioon. (BitLocker Group Policy Settings 2015.)

Käytettävän salaustavan valinta tapahtuu ryhmäkäytännön asetuksella Choose drive encryption method and cipher strength. Asetuksesta on erilliset versiot Windows versioille, jotka tukevat eri salausmenetelmiä. Käytettävän salaustilan voi myös määritellä erikseen käyttöjärjestelmän levylle, kiinteille datalevyille ja ulkoisille medioille.

TPM-piirin käyttö PIN-koodilla valitaan asetuksella Require additional authentication at startup. Tällä asetuksella käyttäjä voi hyväksyä ja kieltää erilaisten TPM-suojauksen toimintatapojen käytön. Kukin yhdistelmä, kuten TPM startup tai TPM startup with PIN, tulee eksplisiittisesti joko sallia tai kieltää. Lisäksi asetuksen ominaisuudella Allow BitLocker without a compatible TPM voidaan kieltää järjestelmälevyn salaus ilman yhteensopivaa TPM-piiriä. TPM-piirin kanssa käytettävien PIN-koodien pituutta ja kompleksisuutta voi lisäksi säädellä asetuksilla Configure minimum PIN length for startup ja Allow enhanced PINs for startup.

Salauksen kanssa käytettäviin palautusmenetelmiin otetaan kantaa asetuksella Choose how BitLocker-protected operating system drives can be recovered. Asetuksen avulla voidaan suoraan kieltää tai sallia sekä palautussalasanan että palautusavaimen käyttö. Asetuksen toinen merkittävä funktio on säädellä palautustietojen tallentamista Active Directory -hakemistoon. Lisäksi sillä voidaan ottaa kantaa myös käyttäjälle näytettäviin palautusvaihtoehtoihin.

6 KONFIGURAATION KOVENTAMINEN

Koventamisella tarkoitetaan IT-järjestelmän potentiaalisen hyökkäyspinta-alan minimoimista korkeamman tietoturvan saavuttamiseksi. Tässä luvussa arvioidaan erilaisten käytännön toimenpiteiden vaikutusta BitLocker-konfiguraation tietoturvaan. Toimenpiteitä voidaan soveltaa erilaisiin korkean tietoturva ympäristöihin, tavoitellusta tietoturvan ja käytettävyyden tasosta riippuen.

6.1 Salausmenetelmän valinta

BitLocker käyttää oletusasetuksilla datan AES-salaukseen 128-bittistä salausavainta. Jos avaimen koko nostetaan 256 bittiin, nousee mahdollisten erilaisten avainten lukumäärä eksponentiaalisesti. Teoriassa siis myös avaimen arvaamiseen tarvittu aika nousee samassa suhteessa.

AES-standardia pidetään yleisesti turvallisena, eikä siihen tunneta murtamistapaa joka olisi nopeampi kuin itse salausavaimen arvaaminen (Bruce Schneier 2012). Koska salauksen nopeus ei enää nykytietokoneilla ole ongelma, ei käyttäjällä ole mitään syytä olla käyttämättä 256-bittistä avainpituutta. Pidemmän avainpituuden käyttö on kuitenkin hyödyllistä vain, jos myös kaikki VMK-avainta suojaavat avaimet ovat todella 256-bittisiä.

Salauksen ketjutustiloissa uudet käyttöjärjestelmät ovat aina siirtyneet käyttämään oletuksena uusinta versiota. Tämä on viisasta myös tietoturvamielessä, sillä uudemmat ketjutustilat Elephant Diffuser ja XTS tehostavat tiedon luottamuksellisuuden varmistamista. Kuitenkin myös vanhempaa CBC-ketjutustilaa pidetään edelleen AES:n kanssa käytettynä turvallisena. (BitLocker: AES-XTS 2016)

6.2 TPM-kirjautumistavan valinta

BitLocker käyttää TPM-piiriä oletuksena ilman erillistä PIN-koodia tai käynnistysavainta. Tällöin TPM-piiri avaa salauksen käynnistyksen yhteydessä automaattisesti, kunhan järjestelmä käynnistyy TPM-piirin luottamaan käyttöjärjestelmään. Jos tietokone yritetään käynnistää toisella käyttöjärjestelmällä tai levy yritetään siirtää toiseen tietokoneeseen, TPM-piiri ei suostu avaamaan VMK-avainta ja tallennettu tieto pysyy vahvasti salattuna. Käyttöjärjestelmän automaattinen käynnistyminen asettaa kuitenkin suuren paineen itse käyttöjärjestelmän tietoturvalle. Tällöin potentiaalinen hyökkäys työasemalle tallennettujen tietojen saamiseksi voitaisiin kohdistaa käyttöjärjestelmän haavoittuvuuksiin. (BitLocker Drive Encryption Step-by-Step Guide 2009.)

Käyttöjärjestelmän turvaaminen onnistuu yksinkertaisimmillaan PIN-koodin lisäämisellä TPM-piirin toimintaan. Tällöin luvaton käyttäjä ei pysty käynnistämään salattua käyttöjärjestelmää ilman PIN-koodia. Vaikka PIN-koodi ei olisi järin monimutkainen, tuo se silti merkittävän lisäyksen tietoturvaan. TPM-piiri nimittäin rajoittaa mahdollisia avausyrityksiä estäen samalla laajat hakemisto- ja brute force -hyökkäykset PIN-koodia kohtaan. Jos levy taas irrotetaan työasemasta, tulisi hyökkääjän selvittää PIN-koodin lisäksi myös TPM-piirin 2048-bittinen RSA-avain. (BitLocker™ Drive Encryption Security Policy 2011, 8.)

Mikäli TPM-piirin turvaksi haluaa todella salaus-avainta vastaavan avaimen, voi sen lisäksi valita myös erillisen käynnistysavaimen. Tällöin TPM-piiri varmistaa käynnistysosion koskemattomuuden, mutta VMK-avaimen avaus vaatii silti todellisen 256-bittisen avaimen. Käynnistysavain luetaan aina suojaamattomalta USB-medialta, joten sen säilyttämiseen tulee kuitenkin kiinnittää erityistä huomiota.

6.3 Palautustapojen valinta

BitLocker lisää salatuille osioille oletuksena numeerisen palautussalasanan. Numeerinen palautussalasana voidaan esimerkiksi tallentaa tekstitiedostossa USB-muistille tai yrityksen Active Directory -hakemistoon. Palautustilanteessa numeerinen salasana riittää sellaisenaan koko salauksen avaamiseen ja se syötetään suoraan BitLockerin käyttöliittymään.

Vaihtoehtona palautussalasanalle tarjotaan palautusavainta, joka on itseasiassa 256-bittinen puhdas avain. Toisin kuin palautussalasana, palautusavain on binäärisessä tiedostomuodossa, eikä sitä voi käyttää tekstimuotoisena. Palautusavain-termi menee helposti sekaisin palautussalasanan kanssa, sillä Microsoft viittaa usein myös omassa dokumentaatiossaan palautusavaimeen, vaikka kontekstissa tarkoitetaan palautussalasanaa.

Palautussalasanassa lopullinen salausavain saadaan muodostamalla käyttäjän syötteestä väliavain ja lisäämällä siihen satunnaisesti generoitu suola. Kuten luvussa 4.3.3 todetaan, tämän palautusavaimen efektiivinen entropia on kuitenkin vain 128 bittiä. Potentiaalinen hyökkääjä voisi siis jonkin 256-bittisen avaimen sijaan pyrkiä arvaamaan 128-bittisen palautusavaimen, ja onnistua avaamaan sillä VMK-avaimen salauksen.

Mikäli käytössä on AES-standardin 256-bittinen avaimenpituus, heikentää palautussalasana avainhierarkian entropian teoriassa 128-bittisen avaimenpituuden tasolle. Mikäli salauksessa halutaan siis käyttää puhtaasti 256-bittisen entropian omaavia avaimia, tulisi palautussalasanan tilalla käyttää 256-bittisiä palautusavaimia.

7 MUUT LEVYNSALAUSTUOTTEET

BitLocker muistuttaa ominaisuuksiltaan monia muita levynsalaustuotteita. Myös esimerkiksi avoimen lähdekoodin VeraCrypt ja Applen FileVault 2 perustuvat paikalliseen sisäkkäiseen avainhierarkiaan. Avaimet generoidaan paikallisesti ja mahdollinen keskitetty hallinta perustuu lähinnä palautusavainten varmuuskopiointiin. VeraCryptin ja FileVault 2:n viimeisimmät versiot käyttävät myös AES-standardia XTS-ketjutustilassa. (VeracCrypt 2014; Apple 2017.)

Yrityksille suunnattujen erillisten levynsalaustuotteiden perusidea on suurien työasemamassojen salauksen helppo keskitetty hallinta. Salaustuotteet kuten Sophos SafeGuard ja Symantec Endpoint Encryption tarjosivat ennen oman sovelluksensa varsinaisen levynsalauksen toteuttamiseen. Oman sovelluksen avulla tuotteet mahdollistivat esimerkiksi käyttäjän salausavaimen sitomisen yrityksen toimialueen käyttäjätunnukseen ja siten automaattisen synkronoinnin vaikkapa useammalle salatulle työasemalle. Samalla salausavaimen käyttöoikeus voitiin sitoa liitetyn tunnuksen voimassaoloon. (Sophos 2016; Symantec 2017.)

Sekä Symantec että Sophos ovat kuitenkin viimeisimmissä versioissaan siirtyneet käyttämään varsinaisessa levynsalauksessa käyttöjärjestelmien omia BitLocker ja FileVault 2 levynsalausmekanismeja. Tuotteet joutuvatkin nykyään toimimaan BitLockerin rajoitteiden puitteissa, eikä esimerkiksi käyttäjäkohtaisten salausavainten synkronointi eri tietokoneiden välillä enää onnistu. (Sophos 2016; Symantec 2017.)

8 POHDINTA

Opinnäytetyön tarkoituksena oli perehtyä BitLocker-levynsalaustuotteen toimintaan ja pohtia miten sen arkkitehtuuri vaikuttaa tuotteen käyttöön tietoturvallisessa ympäristössä. Opinnäytetyön tuloksena saatiin selvitys tuotteen keskeisistä teknisistä ratkaisuista sekä joukko käytännön toimenpiteitä joilla tuotteen tietoturvaan voidaan vaikuttaa. Tulosten avulla BitLockeria voidaan esimerkiksi verrata muihin saatavilla oleviin levynsalaustuotteisiin. Arvioituja koventamistapoja voidaan myös suoraan soveltaa tuotteen käytössä.

Työn tuloksista voidaan todeta, että BitLocker käyttää levynsalaukseen pääosin yleisesti turvalliseksi todettuja mekanismeja. Salausavainten muodostamista luvussa 4.3.3 tarkastellessa kuitenkin huomattiin, että vaikka salaukselle valittaisiin suurempi avainkoko, ei koko avainketjun todellinen entropia välttämättä ole suuremman avainkoon mukainen. Tuotteen tietoturvan korottaminen korkeammalla avaimenpituudella vaatii siis myös käytettyjen avaintyyppien arviointia.

Opinnäytetyö koostui pääosin levynsalauksen peruskäsitteiden selvittämisestä ja BitLocker-tuotteeseen liittyvän dokumentaation tulkitsemisesta. Erityisen haastavaksi osoittautui Microsoftin hajanaisena julkaiseman teknisen dokumentaation löytäminen ja tulkitseminen. Valtaosa BitLocker-tuotteen dokumentaatiosta on julkaistu vain Yhdysvaltojen kansallisen standardi- ja teknologiainstituutin toimesta erinäisten sertifiointien yhteydessä. Dokumentaation tulkitseminen vaati myös odotettua enemmän syventymistä levynsalauksen taustalla olevaan teoriaan.

Vaikka aihealueen laajuus osoittautui opinnäytetyön kannalta ongelmalliseksi, saatiin työn tuloksina arvokasta tuntemusta niin BitLockerin kuin muidenkin levynsalaustuotteiden toiminnasta.

LÄHTEET

H. Delfs, H. Knebl. 2015. Introduction to Cryptography: Principles and Applications. 3. painos. Berlin: Springer-Verlag.

Microsoft Corporation. 2009. TechNet. BitLocker Drive Encryption Step-by-Step Guide. Luettu 11.5.2017. https://technet.microsoft.com/en-us/library/cc732725(v=ws.10).aspx

National Institute of Standards and Technology. 2001. Federal Information Processing Standards Publication 197. Announcing the
Advanced encryption standard (AES). Luettu 3.5.2017. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

Rafal Sosnowski. 2016. TechNet Blogs. BitLocker: AES-XTS. Luettu: 22.5.2017. https://blogs.technet.microsoft.com/dubaisec/2016/03/04/bitlocker-aes-xts-new-encryption-type

National Institute of Standards and Technology. 2016. Block cipher modes. Luettu: 22.5.2017. http://csrc.nist.gov/groups/ST/toolkit/BCM/current_modes.html

Microsoft Corporation. 2006. AES-CBC + Elephant diffuser: A Disk Encryption Algorithm for Windows Vista. Luettu 22.5.2017. https://css.csail.mit.edu/6.858/2012/readings/bitlocker.pdf

Microsoft Corporation. 2007. TechNet Magazine.
Keys to Protecting Data with BitLocker Drive Encryption. Luettu 4.5.2017. https://technet.microsoft.com/en-us/library/2007.06.bitlocker.aspx

Microsoft Corporation. 2011. BitLocker™ Drive Encryption Security Policy. Luettu 27.4.2017. http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1054.pdf

J. Kornblum. 2009. Implementing BitLocker Drive Encryption for Forensic Analysis. Luettu 12.5.2017. http://jessekornblum.com/publications/di09.pdf

Microsoft Corporation. 2017. Trusted Platform Module Technology Overview. Luettu 28.5.2017. https://docs.microsoft.com/en-us/windows/device-security/tpm/trusted-platform-module-overview

Microsoft Corporation. 2013. TechNet. Manage-bde. Luettu 15.5.2017. https://technet.microsoft.com/en-us/library/ff829849(v=ws.11).aspx

Microsoft Corporation. 2014. TechNet. Scripting with Windows PowerShell. Luettu 17.5.2017. https://technet.microsoft.com/en-us/library/bb978526.aspx

Microsoft Corporation. 2012. TechNet. BitLocker Cmdlets in Windows PowerShell. Luettu 17.5.2017. https://technet.microsoft.com/en-us/library/jj649829(v=wps.630).aspx

Microsoft Corporation. 2011. TechNet. Group Policy for Beginners. Luettu 10.5.2017. https://technet.microsoft.com/en-us/library/hh147307(v=ws.10).aspx

Microsoft Corporation. 2015. BitLocker Group Policy Settings. TechNet. Luettu 29.5.2017. https://technet.microsoft.com/en-us/library/jj679890(v=ws.11).aspx

Bruce Schneier. 2012. Can the NSA Break AES?. Luettu 22.5.2017. https://www.schneier.com/blog/archives/2012/03/can_the_nsa_bre.html

VeraCrypt. 2014. Modes of Operation. Documentation. Luettu 29.5.2017. https://veracrypt.codeplex.com/wikipage?title=Modes%20of%20Operation

Apple. 2017. Macin käynnistyslevyn salaaminen FileVaultin avulla. Luettu 29.5.2017. https://support.apple.com/fi-fi/HT204837

Sophos. 2016. Sophos SafeGuard Enterprise. Luettu 29.5.2017. https://www.sophos.com/en-us/medialibrary/PDFs/factsheets/sophossafeguardenterprisedsna.pdf

Symantec. 2017. Symantec Endpoint Encryption. Luettu 28.5.2017. https://www.symantec.com/products/information-protection/encryption/endpoint-encryption

LIITTEET

Liite 1. Esimerkki kovennetusta ryhmäkäytännöstä

Windows Components/BitLocker Drive Encryption

Policy	Setting
Choose drive encryption method and cipher strength (Windows 10 [Version 1511] and later)	Enabled
Select the encryption method for operating system drives:	XTS-AES 256-bit
Select the encryption method for fixed data drives:	XTS-AES 256-bit
Select the encryption method for removable data drives:	XTS-AES 256-bit

Windows Components/BitLocker Drive Encryption/Operating System Drives

Policy	Setting
Allow enhanced PINs for startup	Enabled
Choose how BitLocker-protected operating system drives can be recovered	Enabled
Allow data recovery agent	Enabled
Configure user storage of BitLocker recovery information:	
	Allow 48-digit recovery password
	Allow 256-bit recovery key
Omit recovery options from the BitLocker setup wizard	Disabled
Save BitLocker recovery information to AD DS for operating system drives	Enabled
Configure storage of BitLocker recovery information to AD DS:	Store recovery passwords and key packages
Do not enable BitLocker until recovery information is stored to AD DS for operating system drives	Disabled
Configure minimum PIN length for startup	Enabled
Minimum characters:	10

Policy	Setting
Require additional authentication at startup	Enabled
Allow BitLocker without a compatible TPM (requires a password or a startup key on a USB flash drive)	Disabled
Settings for computers with a TPM:	
Configure TPM startup:	Do not allow TPM
Configure TPM startup PIN:	Allow startup PIN with TPM
Configure TPM startup key:	Do not allow startup key with TPM
Configure TPM startup key and PIN:	Do not allow startup key and PIN with TPM