Bitlocker šifrování disků ve firemním prostředí.

Bc. Karol VAIT

Diplomová práce
2019

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2018/2019

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Karol Vait**
Osobní číslo:	**A17375**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Bitlocker šifrování disků ve firemním prostředí.**
Téma anglicky:	**Bitlocker Disk Encryption in a Corporate Environment.**

Zásady pro vypracování:

1. **Vypracujte literární rešerši na téma šifrování disků.**
2. **Popište princip funkce nástroje Bitlocker a jednotlivé autentizační metody.**
3. **Proveďte rozbor možností centrální správy a Network unlock funkce ve firemním prostředí.**
4. **Otestujte možnosti a způsob nasazení.**
5. **Zhodnoťte výhody a celkové zabezpečení navrženého způsobu řešení.**

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **MULLEN Timothy. Thor's Microsoft Security Bible: A Collection of Practical Security Techniques. United States of America: Elsevier, 2011. ISBN 978-1-59749-572-1.**
2. **Pavel Yosifovich, Mark E. Russinovich, David A. Solomon, Alex Ionescu ./Windows Internals Part 1: System architecture, processes, threads, memory management, and more/. Seventh edition. Redmond: Microsoft, [2017]. ISBN978-0735684188. https://archive.org/details/windows-internals-part1-7th**
3. **RUSSINOVICH, Mark, David A. SOLOMON a Alex IONESCU. Windows Internals: Part 2. 6'th Edition. United States of America: Microsoft Press, 2012. ISBN 978-0-7356-6587-3.**
4. **MINASI, Mark, Kevin GREENE, Robert BUTLER, John MCCABE, Robert PANEK, Michael RICE, Stefan ROTH a Christian BOOTH. Sybex: Mastering Windows Server? 2012 R2. Indianapolis, Indiana: John Wiley & Sons, 2014. ISBN 978-1-118-33172-9.**
5. **WARNER, Timothy a Craig ZACKER. Securing Windows Server 2016: Exam Ref 70-744. United States of America: Pearson Education, 2017. ISBN 978-1-5093-0426-4.**
6. **Microsoft. Windows IT Pro Center: Bitlocker. Bitlocker (Windows 10): Microsoft Docs [online]. 2017. Dostupné z: https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview**

Vedoucí diplomové práce: **doc. Ing. Martin Sysel, Ph.D.**
Ústav počítačových a komunikačních systémů

Datum zadání diplomové práce: **30. listopadu 2018**

Termín odevzdání diplomové práce: **17. května 2019**

Ve Zlíně dne 14. prosince 2018

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové/~~bakalářské~~ práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 17.5.2019 Bc. Karol VAIT, v. r.

ABSTRAKT

Táto diplomová práca sa zaoberá témou šifrovania disku v prostredí Microsoft Windows. Cieľom práce bolo v prvom rade teoreticky popísať princíp, požiadavky, výhody, nevýhody a možnosti centrálnej správy šifrovacieho nástroja Bitlocker a následne na reálnych scenároch otestovať možnosti nasadenia. Zároveň bolo popísané správanie sa systému so šifrovaným diskom v bežnej prevádzke a základné princípy, ktoré by mala organizácia pri nasadení dodržať.

Kľúčové slová: Bitlocker, Network Unlock, Šifrovanie Diskov, Adresárová Služba, Skupinové Politiky, Windows Server.

ABSTRACT

This thesis covers the topic of disk encryption in Microsoft Windows. The aim of the thesis is to describe the principle, requirements, advantages, disadvantages and central management of the Bitlocker encryption tool and then to test the possibilities of deployment on real scenarios. There was also described the behavior of the encrypted disk drive in daily operations and the basic principles that the organization should follow when deployed.

Keywords: Bitlocker, Network Unlock, Disk Encryption, Active Directory, Group Policy, Windows Server.

Poďakovanie

Rád by som sa poďakoval vedúcemu mojej diplomovej práce pánovi doc. Ing. Martinovi Syslovi, Ph.D., za jeho podnetné rady a pripomienky a mojej manželke Kristíne za morálnu podporu pri mojom štúdiu ...

Motto:

„Je iba jediná prekážka na dosiahnutie tvojho cieľa – ty sám.“

neznámy

OBSAH

ÚVOD

V dnešnej „informačnej“ dobe, keď nájdeme počítačom riadené systémy na každom kroku, si pomaly čím ďalej tým viac užívateľov začína uvedomovať, že vo svojom osobnom počítači majú dáta, ktoré by nemali tento systém bez ich vedomia opustiť. Tieto dáta môžu byť naozaj rôznorodé od rodinných fotiek, cez osobné informácie až po citlivé dáta riaditeľa nadnárodnej korporácie. Napriek tomu, že existuje mnoho spôsobov, ako získať tieto dáta bez nutnosti osobného kontaktu, iba za použitia počítačovej siete, je stále množstvo prípadov, kedy je omnoho jednoduchšie daný systém, počítač, či konkrétne pamäťové médium fyzicky odcudziť. Zároveň dnešná uponáhľaná doba, kedy sa ľudia skôr sústredia na to, ako sa čo najrýchlejšie niekam prepraviť, ako na to, že si niekde zabudnú svoj osobný počítač rovnako napomáha k tomu, že ich osobné dáta môžu skončiť v nepovolaných rukách.

Každý moderný operačný systém vo svojej základnej konfigurácii už dnes štandardne ponúka istý stupeň ochrany. Len v minimálnom počte prípadov je však táto konfigurácia dostatočná, ak je fyzicky odcudzený samotný pevný disk, či pamäťové médium. Ako sa teda dá v takýchto situáciách brániť? Odpoveď samozrejme nie je úplne jednoduchá ale dobrý štartovací bod predstavuje šifrovanie diskov. Šifrovanie disku zabezpečí, že dáta sú chránené nielen v prípade, ak útočník odcudzí celý systém, ale aj v prípade, ak sa mu podarí ukradnúť iba samotné šifrované pamäťové médium. Nástrojov na šifrovanie diskov je pritom veľké množstvo od náročných, vysoko profesionálnych, až po voľne dostupné, užívateľsky jednoduché. Cieľom tejto práce je podrobnejšie popísať jeden z týchto nástrojov – nástroj Bitlocker.

V prvých kapitolách teoretickej časti mojej práce sú stručne zhrnuté dôležité fakty a technológie, ktoré so šifrovaním pevných diskov úzko súvisia a šifrovanie, ako také je na nich závislé. Nasledovné kapitoly sa potom priamo zaoberajú Bitlocker nástrojom. Bližšie je popísaná história samotného nástroja, požiadavky na systém aj prípadnú implementáciu v infraštruktúre spoločnosti. Spomenutá je takisto verzia „Bitlocker To Go“, ktorá umožňuje šifrovanie prenosných pamäťových médií. Tak ako každý iný softvérový produkt, aj Bitlocker má svoje výhody a nevýhody oproti iným, konkurenčným produktom. Tieto sú popísané v poslednej kapitole teoretickej časti.

Praktická časť tejto práce sa následne venuje využitiu Bitlocker nástroja v reálnej praxi. Vo virtuálnom prostredí na platforme Microsoft Hyper-V sú popísané funkcie a nevyhnutné konfigurácie jednotlivých systémov a ich komponentov. Nasledovné kapitoly potom na týchto

systémoch demonštrujú možnosti centrálnej správy a vybrané scenáre nasadenia, ich špecifiká, zabezpečenie, výhody a nevýhody. Posledné kapitoly sa venujú témam spojeným s každodennou správou systémov so šifrovaným diskom a popisujú správanie týchto systémov v bežnej praxi.

TEORETICKÁ ČASŤ

1 ZÁKLADNE POJMY PRI ŠIFROVANÍ DÁT NA PEVNOM DISKU

1.1 Šifrovanie

Šifrovanie je súbor metód a postupov, pri ktorom sa prevádza otvorený text, pomocou zvoleného šifrovacieho algoritmu na text šifrovaný. Cieľom je znemožniť potenciálnemu útočníkovi získať informácie, ktoré sú obsiahnuté v prenášanej správe. Na druhej strane však musí byť adresát schopný šifrovanú správu korektne previesť späť na otvorený text a to bez straty prenášanej informácie [1, 7].

Šifrovacie algoritmy sa delia na dve základné skupiny

- **Symetrické** – využívajú rovnaký šifrovací a dešifrovací kľúč. Táto ich vlastnosť zároveň napovedá, čo bude najväčšou slabinou symetrickej šifry – uchovávanie a distribúcia kľúča medzi odosielateľom a adresátom. Veľkou výhodou je však rýchlosť, čím je tento typ veľmi vhodný na šifrovanie veľkého objemu dát.

  AES (Advanced Encryption Standard) je jednou z najpoužívanejších blokových symetrických šifier využívaných v systémoch šifrovania pevných diskov.

  „AES je prvá šifra dostupná širokej verejnosti, ktorá bola zároveň uznaná Národnou bezpečnostnou agentúrou NSA k šifrovaniu najtajnejších dokumentov. V roku 2002 začala byť k svojmu účelu používaná ako federálny štandard USA“ [8].

  Šifra má pevne danú veľkosť bloku 128 bitov a veľkosti kľúčov 128, 192, a 256 bitov [8].

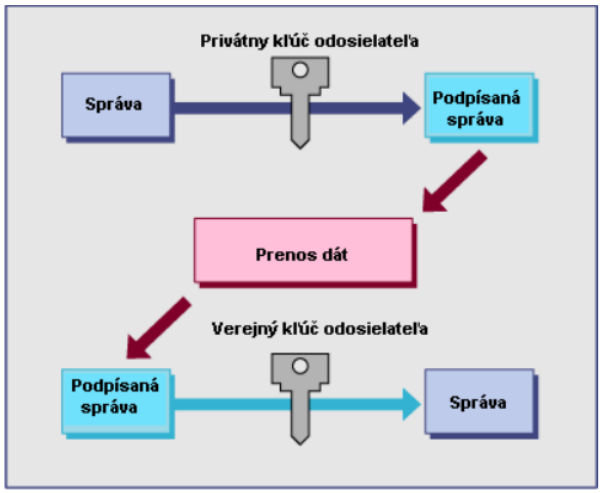
  "*Ak by ste chceli hrubou silou prelomiť 128-bitový kľúč AES, každý z približne 7 miliárd ľudí na Zemi by musel skúšať 1 miliardu kľúčov za sekundu po dobu 1,5 trilióna rokov, aby sa vyskúšali všetky kľúče” [9].*

  Nástroj Bitlocker používa AES šifrovanie v dvoch odlišných módoch:

  - CBC (Cipher Block Chaining) - predstavuje režim, kedy sa na bloky otvoreného textu aplikuje funkcia XOR. Použitie CBC zabezpečuje, že rovnaké údaje v rôznych sektoroch nám po šifrovaní poskytnú rôzny výstup.
  - XTS (XEX - Based Tweaked - Codebook Mode) – v tomto režime sa stále vykonáva medzi blokmi XOR funkcia, ale zároveň sa pridáva ďalší kľúč. Týmto kľúčom môže byť adresa sektoru, príp. jeho index, čo zvyšuje počet možných permutácií.

  Obidva módy podporujú 128 a 256bit veľkosť kľúča [10].

- **Asymetrické –** na rozdiel od symetrických šifier sa pri asymetrických šifrách využívajú dva rozdielne kľúče (verejný a súkromný kľúč). Tieto sú navzájom od seba neodvoditeľné. Asymetrická šifra je vo svojej podstate rádovo pomalšia ako symetrická a nie je tak najvhodnejšou voľbou na šifrovanie veľkého objemu dát. V praxi sa preto veľmi často využíva kombinácia oboch týchto šifier – symetrická šifra na zašifrovanie veľkého objemu dát a asymetrická šifra na zašifrovanie kľúčov symetrickej šifry.



Obr. 1: Symetrická kryptografia [11].

1.2 Hashovanie

Hash, alebo aj digitálny odtlačok je funkcia, ktorá zabezpečuje prevod ľubovoľne dlhého vstupného reťazca na výstupný, ľahko vypočítateľný reťazec definovanej dĺžky. Dĺžku výstupného reťazca pritom určuje sila použitého hashovacieho algoritmu. Aktuálne najpoužívanejšími sú Secure Hash Algorithm (SHA) druhej generácie, s veľkosťou 224 až 512 bitov.

Najdôležitejšími vlastnosťami hash funkcií sú:

- **Jednoduchosť, rýchlosť, široké možnosti využitia** – detekcia chýb pri prenose, modifikácie uložených dát, filtrovanie dát, atď....
- **Odolnosť proti kolízii** – rôzne vstupné dáta majú vždy inú hodnotu hash, rovnaké vstupné dáta majú rovnakú hodnotu hash. Aj malá zmena vo vstupných dátach spôsobí výraznú zmenu vo vypočítanom hash.
- **Jednosmernosť** – z hash reťazca nie je možné získať vstupný reťazec [7, 12].

1.3 Autentifikácia

„*Autentifikácia je proces, pri ktorom používateľ systému dokazuje vlastníctvo konkrétnej digitálnej identity. Po úspešnej autentifikácii vzniká prepojenie medzi používateľom a danou digitálnou identitou. Existujú tri základné spôsoby, ako sa môže používateľ preukázať:*

- ***Niečo, čo používateľ pozná*** *– používateľské meno a k nemu prislúchajúce heslo, odpoveď na „bezpečnostnú otázku“ a iné.*
- ***Niečo, čo používateľ vlastní*** *– fyzické zariadenie, ako je platobná karta, USB token, či smart karta.*
- ***Niečo, čím používateľ je*** *– patria sem biometrické údaje, ako napr. odtlačky prstov, snímanie očnej dúhovky, hlasu, dlane“ [14].*

Autentifikáciu najčastejšie rozdeľujeme na **jednofaktorovú** a **dvojfaktorovú**. Pri dvojfaktorovej autentifikácii musí užívateľ použiť minimálne dva z vyššie uvedených spôsobov autentifikácie súčasne [7, 13, 14].

1.4 Autorizácia

Je väčšinou po predchádzajúcej autentifikácii ďalším krokom, kde sa rozhoduje, či daný užívateľ alebo zariadenie, majú prístup k požadovaným zdrojom či službám. Zjednodušene povedané v tejto fáze sa rozhoduje o tom, čo všetko môže žiadateľ s daným prostriedkom robiť.

Prístupové práva v prostredí Microsoft operačných systémov sa štandardne prideľujú na základe:

- **Definovanej skupiny** – skupina užívateľov s rovnakými požiadavkami na prístup k jednému alebo viacerým zdrojom.
- **Pridelenej role** – každá rola má definované špecifické oprávnenia v danom systéme. Užívateľ môže mať pridelenú jednu alebo viacero rolí na základe ktorých následne získava oprávnenia definované pre danú rolu.
- **Individuálneho prístupu** – každý užívateľ má definované svoje špecifické oprávnenia [13, 14].

2 MOŽNOSTI ŠIFROVANIA DÁT NA PEVNOM DISKU

- Šifrovanie celého disku (FDE)

Ide o spôsob šifrovania, kedy je zašifrovaný celý obsah pevného disku, vrátane dočasných a systémových súborov, či zavádzacieho oddielu.

Nespornou výhodou tohto riešenia je, že po prvotnom zašifrovaní celého disku, sú automaticky chránené všetky dáta na pevnom disku. Užívateľ preto nemusí riešiť dilemu, či konkrétne dáta sú citlivé a treba ich zašifrovať, alebo nie. Vo firemnom prostredí takto odpadá mnoho problémov s konfiguráciou rôznych šifrovaných úložísk na koncových staniciach. Pri notebookoch, ako aj iných prenosných zariadeniach so zapnutým FDE, sa rapídne znižuje riziko zneužitia firemných dát pri strate, či odcudzení takéhoto zariadenia.

Nevýhodou tohto riešenia môže byť pri pomalších hardvérových konfiguráciách rýchlosť prístupu k uloženým dátam. Zároveň si treba uvedomiť, že dáta nie sú chránené pri prenose po sieti, ani pri vzdialenom prístupe cez sieť – ak užívateľ na danom disku pracuje.

- Šifrovanie vybraných dát (FES)

Šifrovaním konkrétnych alebo aj vybraných dát sa väčšinou rozumie šifrovanie jednotlivých súborov, zložiek alebo celých diskových oddielov. Príkladom môžu byť rôzne šifrované archívy alebo v Microsoft operačných systémoch, systém šifrovaných súborov (EFS) [15].

Tento prístup kladie zvýšené nároky na užívateľa a kľúčovou sa tu stáva určitá disciplína. Užívateľ musí dáta, ktoré majú byť chránené ukladať do presne definovaných šifrovaných úložísk, alebo jednotlivé dáta priebežne šifrovať.

Za výhodu v tomto prípade môžeme považovať celkovo nižšie nároky na hardvérové vybavenia, ako v prípade šifrovania celého disku. Väčšina z týchto metód zároveň rieši problémy popisované vyššie, kedy dáta neboli chránene pri prenose po sieti, príp. pri vzdialenom pripojení cez sieť [15].

Za špecifickú formu tohto typu šifrovania môžeme považovať možnosť Bitlocker nástroja, kedy sú na pevnom disku automaticky šifrované iba bloky, ktoré obsahujú uložené dáta. Voľné bloky ostávajú nešifrované. Pri použití tejto možnosti si však treba dať pozor, pretože ak boli na pevnom disku zmazané nejaké dáta, pred aktivovaním samotného šifrovania, tak tieto ostanú na disku v nešifrovanej podobe.

2.1 Hardvérové šifrovanie

Šifrované pevné disky (SED - Self Encryption Drives) – sú moderné pevné disky, so vstavanými šifrovacími funkciami. O šifrovanie dát uložených na disku sa stará elektronika samotného disku. Väčšinou sa jedná o AES šifrovanie, zabezpečované AES koprocesorom [16].

SED disky boli na trhu dostupné už niekoľko rokov, ale spoločnosť Microsoft nemohla podporiť ich používanie s niektorými staršími verziami systému Windows, pretože disky neobsahovali dôležité funkcie pre správu kľúčov. Microsoft spolupracoval s dodávateľmi na zlepšení hardvérových schopností a nástroj BitLocker teraz podporuje ďalšiu generáciu zariadení SED, ktoré sa nazývajú šifrované pevné disky. Tieto disky zvyšujú výkon systému tým, že presúvajú kryptografické výpočty z procesora počítača na riadiace obvody samotného disku. Zároveň by mali byť odolnejšie voči rôznym typom útokom, ktorými trpia softvérový konkurenti [6, 16].

Aj v prípade hardvérového šifrovania je nevyhnutné si vopred overiť, či disk spĺňa špecifikáciu a nie je náchylný k zneužitiu.

Možné problémy

Pod operačným systémom Windows nástroj Bitlocker v prípade, že zistí prítomnosť pevného disku, ktorý podporuje hardvérové šifrovanie, sa automaticky snaží využiť tento typ šifrovania. V podstate by sa to mohlo zdať ako logický krok. Problém je však v tom, že užívateľ nijakým spôsobom nebol upozornený, že sa softvérové šifrovanie vôbec nepoužije. Situácia sa čiastočne zmenila po tom, čo koncom roku 2018 Randbound Univerzita zverejnila výskum ohľadom zraniteľností, ktoré boli zistené u vybraných modelov diskov popredných výrobcov (obrázok nižšie, uvádza výrobcu a konkrétny model, ako aj nájdený typ zraniteľnosti). Z dôvodu nedodržania špecifikácie, bola kompromitovaná bezpečnosť uložených dát. Na základe tohto výskumu, bolo vydané odporúčanie, aby sa na týchto diskoch z dôvodu bezpečnosti radšej využívalo softvérové šifrovanie. Spoločnosť Microsoft k tomuto problému zverejnila postup, ako štandardné správanie Bitlocker nástroja zmeniť a aj v prípade, že bol zistený pevný disk s podporou hardvérového šifrovania, naďalej využívať šifrovanie softvérové.

Drive	1	2	3	4	5	6	7	8	9	Impact
Crucial MX100 (all form factors)	✗	✗	✗							✗ Compromised
Crucial MX200 (all form factors)	✗	✗	✗							✗ Compromised
Crucial MX300 (all form factors)	✓	✓	✓		✗	✓	✓	✓	✓	✗ Compromised
Samsung 840 EVO (SATA)	✗	✓	✓		✓	✓	✓	✗	✓	~ Depends
Samsung 850 EVO (SATA)	✗	✓	✓		✓	✓	✓	✓	✓	~ Depends
Samsung T3 (USB)				✗						✗ Compromised
Samsung T5 (USB)				✗						✗ Compromised

[1] Cryptographic binding in ATA Security (High mode)
[2] Cryptographic binding in ATA Security (Max mode)
[3] Cryptographic binding in TCG Opal
[4] Cryptographic binding in proprietary standard
[5] No single key for entire disk
[6] Randomized DEK on sanitize
[7] Sufficient random entropy
[8] No wear leveling related issues
[9] No DEVSLP related issues

Obr. 2: Prehľad zistených problémov na SSD diskoch [17].

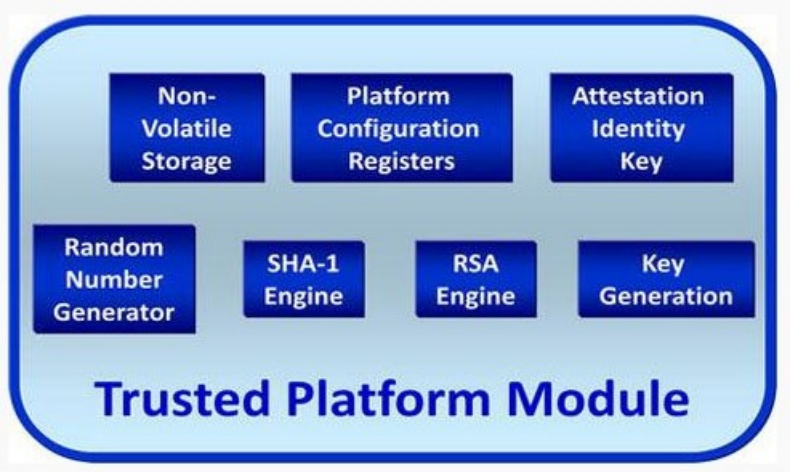
2.1.1 **TPM čip**

Trusted Platform Module (TPM) je kryptografický hardvérový modul, ktorý dokáže bezpečne ukladať artefakty používané na overenie platformy (počítač alebo prenosný počítač). Tieto artefakty môžu obsahovať heslá, certifikáty alebo šifrovacie kľúče. Modul TPM zároveň pomáha zabezpečiť integritu danej platformy (napr. proces zavádzania systému) [18].

Samotná špecifikácia TPM je definovaná, vyvíjaná, publikovaná a udržiavaná organizáciou Trusted Computing Group (TCG). TCG taktiež zverejňuje špecifikáciu TPM ako medzinárodnú normu ISO / IEC 11889 [18].

TPM čip je v dnešnej dobe štandardnou súčasťou ako klientských, tak aj servrových systémov a to v podobe čipu, ktorý je fyzicky inštalovaný na základnej doske. Najčastejšie používanými verziami sú dnes TPM verzie 1.2 a TPM verzie 2.0. Najväčšou výhodou novšej špecifikácie je jednoznačne podpora novších šifrovacích algoritmov [19].

Medzi základné komponenty TPM patria:



Obr. 3: Základné komponenty TPM [20].

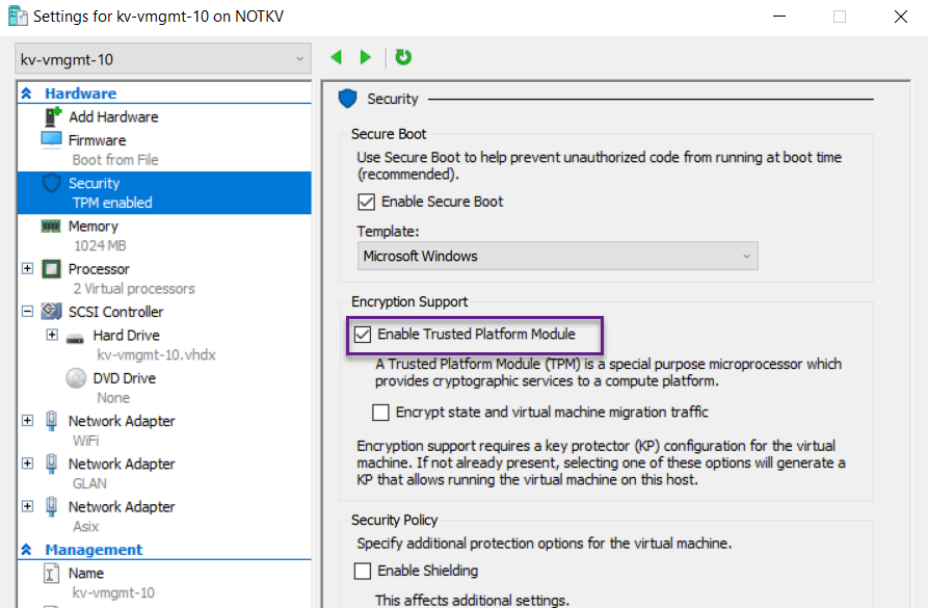
- „***Generátor náhodných čísiel (Random Number Generator)*** *- náhodné čísla sa primárne používajú na zabezpečenie komunikácie medzi žiadajúcou entitou a TPM. Zároveň je však možné požiadať TPM o náhodné číslo aj na iné účely, ako je napríklad šifrovanie a zabezpečenie externých kanálov.*
- ***SHA-1 engine*** *– je hash generátor používaný pre rôzne procesy autorizácia a autentifikácie.*
- ***RSA Engine a Key Generation*** *– TPM používa RSA symetrický algoritmus pre šifrovanie a digitálny podpis. Generátor kľúčov následne využíva tento algoritmus na generovanie asymetrických kľúčov (verejný kľúč a súkromný kľúč). Súkromný kľúč je udržiavaný interne (teda je známy len TPM). Verejný kľúč používa jednotka na šifrovanie údajov, ktoré môžu byť dešifrované iba osobou so súkromným kľúčom (TPM). RSA engine používa kľúče na šifrovanie a dešifrovanie správ a údajov“ [20].*
- *„**Konfiguračné registre platformy** (PCR - Platform Configuration Registers) – je špeciálna časť v TPM pamäti, ktorá má niekoľko unikátnych vlastností. Napríklad PCR od 0 do 7 majú všeobecne definovanú hodnotu po zavádzacom procese - pri načítaní operačného systému. Pri zmene hardvéru, firmvéru alebo zavádzača štartovacej sekvencie operačného systému, sa táto zmena premietne do hodnôt PCR registrov. Systém Windows 10 využíva túto schopnosť na sprístupnenie určitých kryptografických kľúčov iba v presne definovaných časoch počas zavádzacieho procesu“ [21].*
- *„**Stála pamäť** (**Nonvolatile storage**) – je úložiskom, ktorého obsah ostáva zachovaný aj po strate napájania počítača“ [20].*

2.2 Softvérové šifrovanie

Pod pojmom softvérové šifrovanie rozumieme šifrovanie dát s použitím softvérových nástrojov. V tomto prípade nie je potrebné, aby samotný hardvér podporoval nejakú formu šifrovania. Celý proces zabezpečuje softvér, ktorý sa podľa požiadaviek klienta nainštaluje do operačného systému, prípadne vloží časť svojho kódu priamo do zavádzača daného operačného systému. Následne zašifruje súbory, zložky, celý disk, použité miesto na pevnom disku, prípadne prenosné média.

2.2.1 Virtuálny TPM

Virtuálne servery a stanice sú v dnešnej dobe na vzostupe a preto bude čím ďalej tým nevyhnutnejšie, aby aj tieto systémy spĺňali požadovaný stupeň zabezpečenia. S nástupom nových verzii Windows operačných systémov (Windows Server 2016 a novších) preto aj Microsoft prichádza so zaujímavými novými funkciami. Jednou z nich je napríklad Virtuálny TPM čip.



Obr. 4: Virtuálny TPM modul na Microsoft Hyper-V, vlastný zdroj.

Tato nová funkcionalita umožňuje, využiť technológie ktoré vyžadujú TPM čip priamo vo virtuálnom serveri, či stanici. Ak fyzický virtualizačný server TPM čip obsahuje, potom je tento publikovaný do virtuálneho systému. Výhodou je, že virtuálny server vie TPM použiť aj v prípade, že modul nie je fyzicky nainštalovaný vo virtualizačnom serveri. V tomto prípade však musíme počítať s istým kompromisom, čo sa týka bezpečnosti [5].

3 BITLOCKER

„Údaje v stratenom, alebo ukradnutom počítači sú náchylné na neoprávnený prístup a to hlavne formou rôznych špecializovaných softvérových nástrojov, alebo rovno fyzickým presunutím pevného disku z počítača obeti, do iného počítača. Nástroj BitLocker pomáha zamedziť neoprávnenému prístupu k údajom tým, že zabezpečuje ochranu súborov a systémov. Dátové disky šifrované nástrojom Bitlocker, takisto rieši a situácie, kedy by mohlo dôjsť k neoprávnenému prístupu pri nevhodnom spôsobe recyklácie, alebo pri nesprávnom systéme vyradzovania zastaraných počítačov z prevádzky“ [6].

3.1 História a súčasnosť

Prvé verzie nástroja Bitlocker, predstavené v systéme Windows Vista, boli značne obmedzené a dokázali šifrovať iba disky operačného systému. Funkcie zavedené v systéme Windows Vista SP1 a Windows Server 2008 následne pridali podporu pre šifrovanie ostatných pevných dátových jednotiek. V ďalších edíciách boli postupne pridávané nové zaujímavé funkcie, ako napríklad príchod Bitlocker To Go vo Windows 7, alebo nové ochranné mechanizmy vo Windows 8.

S príchodom Windows 10 (verzia 1511) sa Bitlocker posúva na vyššiu bezpečnostnú úroveň, keď Microsoft pridáva podporu XTS AES šifrovacieho algoritmu. Algoritmus spĺňa FIPS štandard a podporuje 128 aj 256bit dĺžku kľúča. Zároveň však algoritmus nie je použiteľný v starších verziách operačného systému Windows. Takisto sa odporúča, aby sa nepoužíval na šifrovanie prenosných médií. Tu sú naďalej preferovanými AES-CBC 128 bit, alebo AES-CBC 256 bit [22, 23].

3.2 Popis

„*Windows BitLocker Drive Encryption je funkcia pre ochranu dát, ktorá je k dispozícii v systéme Windows Vista a novší a vo všetkých edíciách systému Windows Server od verzie 2008. Tento nástroj predstavuje novú funkciu od spoločnosti Microsoft a umožňuje reagovať na reálne hrozby odcudzenia dát, alebo zverejnenia dát v prípade straty, odcudzenia alebo nezodpovedajúceho vyradenia počítačového hardvéru.*

Táto funkcia optimálne využíva technológiu Trusted Platform Module (TPM) na ochranu dát a umožňuje zaistiť, aby s počítačom, v ktorom je prevádzkovaný systém, nebolo možné neoprávnene manipulovať v čase, kedy je systém vypnutý.

Nástroj Windows BitLocker Drive Encryption ponúka rozšírené šifrovanie dát vďaka kombinácii dvoch hlavných čiastkových funkcií: úplné šifrovanie jednotky a kontrola integrity súčastí používaných v prvých fázach spúšťania systému“ [24].

Na čo sa teda nástroj Bitlocker dá použiť:

- Ochrana dát ak je systém
  - vypnutý.
  - odcudzený, alebo stratený.
- Kontrola integrity štartovacieho procesu.

Na čo nástroj Bitlocker naopak nie je vhodný:

- Ochrana dát
  - na zapnutom systéme.
  - pri prenose dát po sieti [6].

3.3 Licencovanie a dostupnosť

Bitlocker je súčasťou vybraných edícií operačného systému Microsoft Windows

- Windows Vista a Windows 7 – edície Ultimate a Enterprise.
- Windows 8 a 8.1 – edície Profesional a Enterprise.
- Windows 10 – edície Profesional, Enterprise a Education.
- Windows server 2008 a novší [25].

Ak organizácia nepotrebuje centrálnu správu nástroja Bitlocker, nie je potrebná žiadna dodatočná licencia a stačí podporovaná edícia Microsoft Windows operačného systému. Častejšie sa však vo firemnom prostredí práve táto funkcionalita považuje za kľúčovú a preto je vhodné použiť nástroj pre centrálnu správu - MBAM. Tento je súčasťou balíka MDOP, ktorý je dostupný iba pre zákazníkov, ktorí majú zakúpenú požadovanú licenciu, resp. spadajú do požadovaného licenčného programu spoločnosti Microsoft.

3.4 Hardvérové Požiadavky

Tak ako každý softvérový nástroj, aj Bitlocker má isté požiadavky, ktoré musí spĺňať systém na ktorom chce používateľ plne využívať všetky výhody tohto nástroja. Nižšie sú uvedené základné parametre, ktoré musia najdôležitejšie komponenty spĺňať.

TPM čip

Aby mohol BitLocker používať modul Trusted Platform Module (TPM), musí mať počítač TPM minimálne verzie 1.2 alebo novší. Ak počítač TPM modul nemá, aktivácia nástroja BitLocker vyžaduje, aby bol štartovací kľúč uložený na prenosnom pamäťovom médiu, ako je napríklad USB kľúč.

- Počítač s TPM musí obsahovať BIOS alebo UEFI rozhranie kompatibilné s Trusted Computing Group (TCG).
- Počítač bez TPM nevyžaduje firmvér kompatibilný s TCG [6].

BIOS, alebo UEFI rozhranie

Systémový BIOS, alebo UEFI rozhranie, musí podporovať triedu veľkokapacitných pamäťových USB médií, ktoré musia zároveň podporovať čítanie malých súborov na USB pamäťovom médiu v prostredí, ešte pred naštartovaním samotného operačného systému [6].

Pevný disk

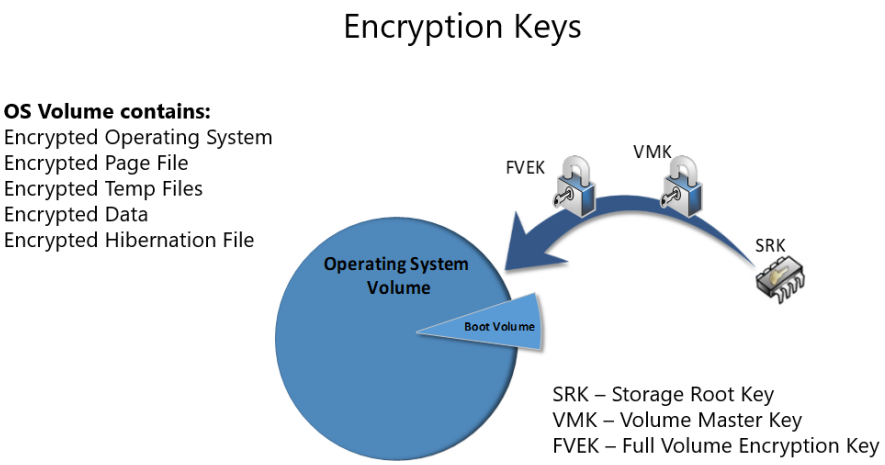
Pevný disk musí byť rozdelený na minimálne dva diskové oddiely:

- **Disk na ktorom sa nachádza samotný operačný systém** – obsahuje operačný systém a všetky podporné súbory. Musí byť naformátovaný systémom súborov NTFS.
- **Systémový disk** – obsahuje súbory, ktoré sú nevyhnutné k načítaniu Windows operačného systému po tom, ako firmvér pripravil systémový hardvér. Tento disk musí byť naformátovaný systémom súborov FAT32, ak systém využíva UEFI, alebo použitím NTFS v prípade BIOS rozhrania. Bitlocker na tomto disku nie je aktívny. Odporúčaná veľkosť disku je minimálne 350MB.

Po nainštalovaní na nový počítač, si Windows operačný systém automaticky vytvorí oblasti, ktoré si nástroj Bitlocker vyžaduje [6].

3.5 Princíp šifrovania

Princíp šifrovania je založený na využití rôznych šifrovacích kľúčov.



Obr. 5: Bitlocker šifrovacie kľúče [26].

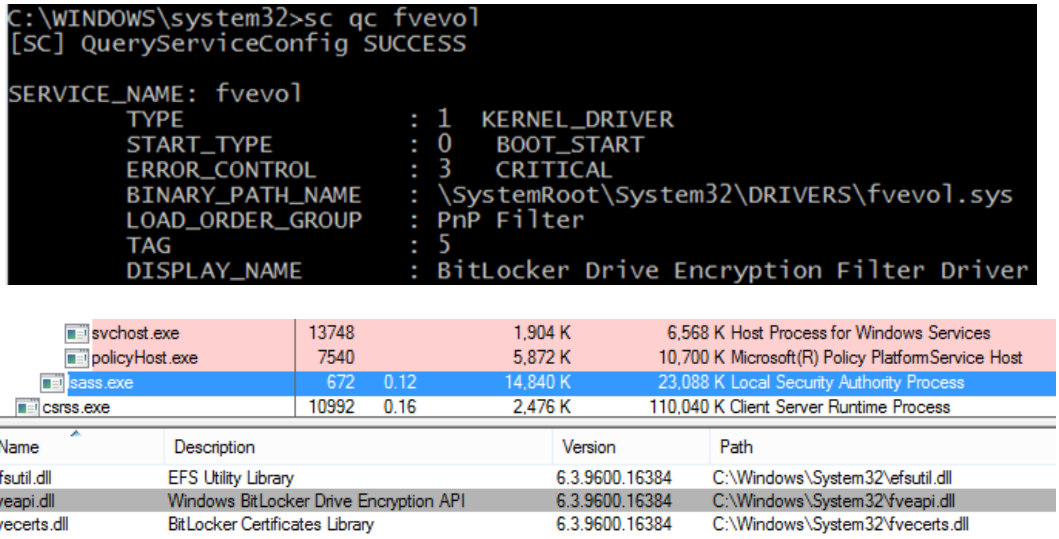
Použité šifrovacie kľúče:

- **SRK** – nachádza sa v TPM.
- **VMK** – šifruje FVEK a je chránený podľa konfigurácie TPM modulom, PIN kódom, alebo uložený na USB prenosnom disku.
- **FVEK** – šifrovaný SRK kľúčom a uložený na pevnom disku pod operačným systémom.
- **CLEAR („Čistý“) –** *„je špeciálny typ kľúča. Tento kľúč sa používa vtedy, keď je Bitlocker ochrana vypnutá, alebo pozastavená – najčastejšie ak prebieha aktualizácia operačného systému, alebo BIOS subsystému. V tejto chvíli neprebieha žiadna autentizácia, ani kontrola integrity daného systému. Je vygenerovaný symetrický šifrovací kľúč (CLEAR), ktorý je uložený na pevnom disku v nezašifrovanej podobe a je ním zašifrovaný VMK. VMK kľúč je takto voľne dostupný a jednoducho dešifrovateľný. Po opätovnom povolení ochrany je CLEAR kľúč odstránený a VMK je znovu zašifrovaný a chránený“ [27].*

Pri aktivácii Bitlocker nástroja sa na pevnom disku (oddiel s operačným systémom) každý sektor šifruje individuálne, pričom sektory označené ako zlé sa nešifrujú. Časť šifrovacieho kľúča je odvodená od samotného čísla sektoru. To znamená, že dva sektory obsahujúce identické nešifrované dáta, budú mať za následok rôzne šifrované bajty. Každý sektor je šifrovaný použitím FVEK šifrovacieho kľúča. Tento kľúč je následne zašifrovaný kľúčom VMK a uložený na disku spolu s odpovedajúcimi metadátami [26, 27].

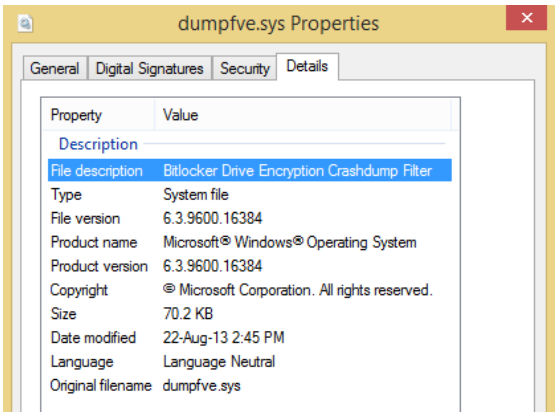
Bitlocker ochranu na pevnom disku môže zapnúť iba správca daného systému. Po povolení šifrovania sú pri prvom reštarte systému vykonané testy, či sú splnené všetky podmienky, aby mohol proces šifrovania disku začať. Ak všetky testy prebehnú úspešne, po následnom naštartovaní operačného systému, sa na pozadí začne proces šifrovania [26, 27].

Po úspešnom zapnutí ochrany sú dáta permanentne šifrované. Operačný systém, konkrétne nízko-úrovňový ovládač súborového systému fvevol.sys, kontroluje generovanie a správu kľúčov. Všetky potrebné dáta sú šifrované a dešifrované transparentne na pozadí bez toho, aby to užívateľ zaznamenal [2, 3, 26, 27].



Obr. 6: Nízko-úrovňový ovládač súborového systému – fvevol.sys [26].

V prípade, že fvevol.sys ovládač spôsobí pád systému (BSOD), obsahuje operačný systém ďalší nízko-úrovňový ovládač dumpfve.sys, zodpovedný za spravovanie výpisu pamäte v prípade pádu systému. Ovládač zabezpečí, aby bol výpis kompletne uložený na disk [3, 26].



Obr. 7: Nízko-úrovňový ovládač súborového systému – dumpfve.sys [26].

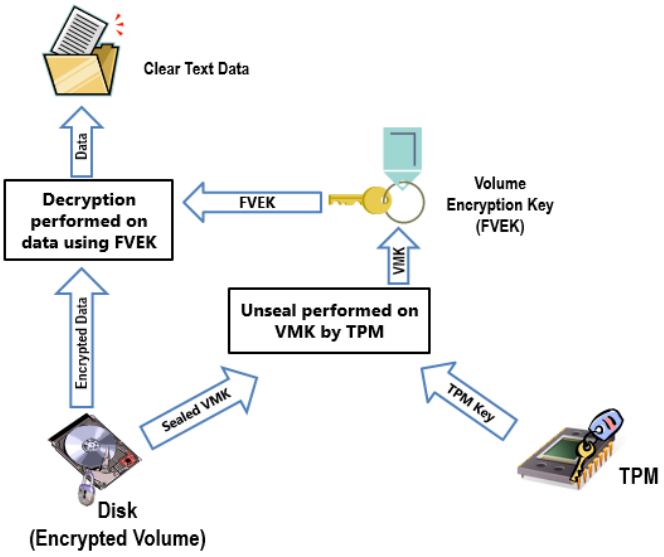
3.5.1 Metódy pre ochranu šifrovacích kľúčov

Bitlocker šifrovanie diskov využíva rôzne metódy na ochranu svojich šifrovacích kľúčov. Podľa zvolenej konfigurácie, môže byť ochrana od jednoduchej, až po využitie viac-faktorovej varianty napr. TPM + PIN.

Rovnako platí, že niektoré typy ochrany je možné využiť iba pre diskový oddiel, na ktorom sa nachádza operačný systém (TPM, TPM + PIN, TPM + USB, TPM + PIN + USB, USB štartovací kľúč). Automatické odomykanie (Auto Unlock) a SmartCard certifikáty, je práve naopak možné využiť iba v prípade dátových diskových oddielov. Všetky ostatné typy ochrany sú pre oba diskové oddiely spoločné.

Typy ochrany (alebo Ochrancov, tzv. Protectors) môžeme rozdeliť nasledovne:

- **TPM modul** – kľúč je uložený v TPM



Obr. 8: Protector – TPM [28].

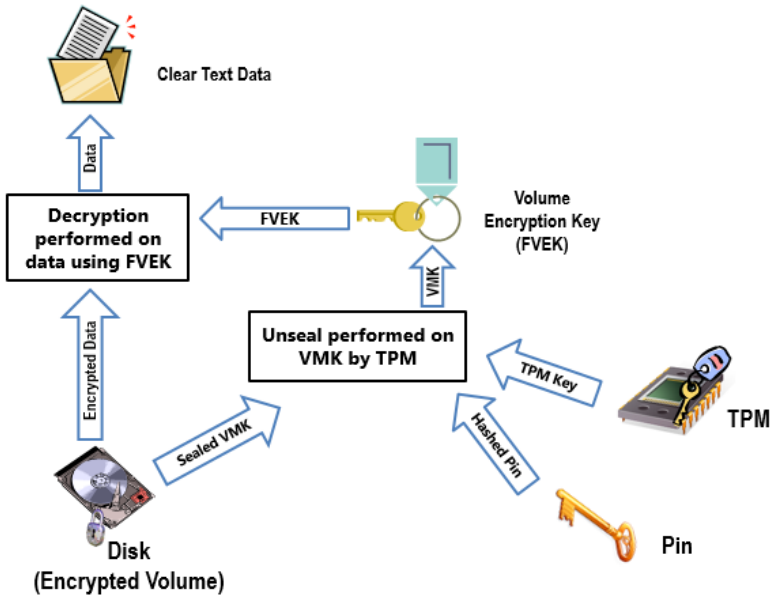
Systémový zväzok systému Windows je šifrovaný pomocou šifrovacieho kľúča FVEK. FVEK je šifrovaný pomocou VMK. VMK je viazaný na TPM čip na základnej doske. Počas procesu zavádzania systému, TPM vykoná počiatočnú validáciu. VMK sa použije na dešifrovanie FVEK, ktorý sa následne využije na dešifrovanie a šifrovanie údajov na zväzku, kde je uložený operačný systém [28].

- **TPM + PIN –** pridáva podporu autentifikácie ešte pred štartom samotného operačného systému (tzv. pre-boot authentication). Užívateľ musí zadať správny PIN, aby sa začal

proces zavádzania operačného systému. V tomto prípade sa jedná o viac-faktorové overovanie.

Rozdelenie PIN kódov

- Štandardný PIN - môže obsahovať 4 až 20 znakov a jeho minimálna dĺžka môže byť konfigurovaná centrálne pomocou skupinových politík.
- Rozšírený PIN – môže obsahovať 4 až 20 alfanumerických znakov a musí byť povolený prostredníctvom skupinových politík (Allow enhanced PINs for startup).



Obr. 9: Protector – TPM + PIN [28].

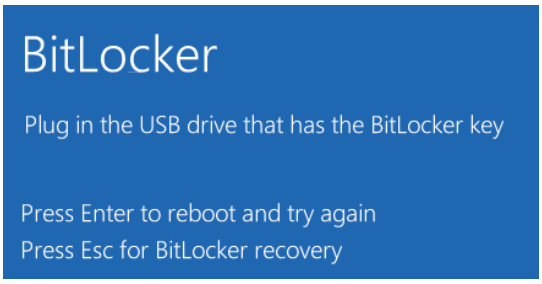
Počas procesu zavádzania TPM vykoná počiatočnú validáciu systému a potom využíva PIN zadaným užívateľom na odblokovanie VMK. VMK sa použije na dešifrovanie FVEK, ktorý sa následne podľa potreby využíva na šifrovanie a dešifrovanie súborov [28].

- **Heslo pre operačný systém (Password Only for OS)** – pracuje podobne ako heslo pre dátové disky (uvedené vyššie). Táto možnosť bola pridaná vo Windows 8. Umožňuje využívať autentifikácie ešte pred štartom samotného operačného systému bez toho, aby musela byť použitá metóda TPM + PIN [26].

- **SmartCard certifikáty –** ako ochrana sa dajú využiť aj certifikáty umiestnené na čipových kartách obsahujúcich štandardné OID (OID = 1.3.6.1.4.1.311.67.1.1). Karty Smartcard možno používať iba s pevnými a USB dátovými jednotkami (nie OS) [26].
- **Automatické odomknutie (Auto-unlock)** – umožňuje užívateľom získať prístup k dátovému disku bez toho, aby zakaždým musel zadávať heslo. Kľúče sú viazané na konkrétneho používateľa (príp. počítač), takže nie je možné ich nakopírovať do iného počítača a povoliť tak prístup.

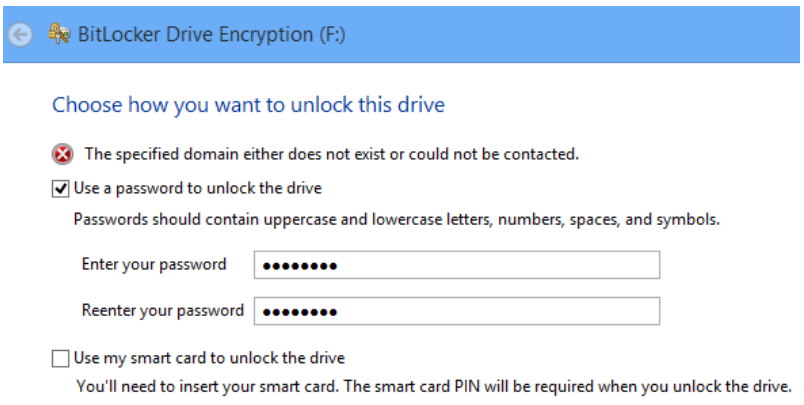
  Konfigurácia sa vykonáva pomocou záznamov v registry databáze:

  - Pevné dátové disky:
    HKLM\SYSTEM\CurrentControlSet\Control\FVEAutoUnlock*
  - Prenosné disky:
    HKCU\Software\Microsoft\Windows\CurrentVersion\FveAutoUnlock* [26].
- **USB štartovací kľúč –** kľúč je uložený na USB pamäťovom médiu, ktoré je nevyhnutné k odomknutiu disku.



Obr. 10: Protector – USB Štartovací kľúč [26].

- **Heslo** – pomocou doménových skupinových politík je možné definovať požiadavky na komplexnosť hesla. Podmienkou však je, aby bol doménový radič dosiahnuteľný. Minimálna dĺžka hesla je 8 znakov [26].



Obr. 11: Protector – Heslo [26].

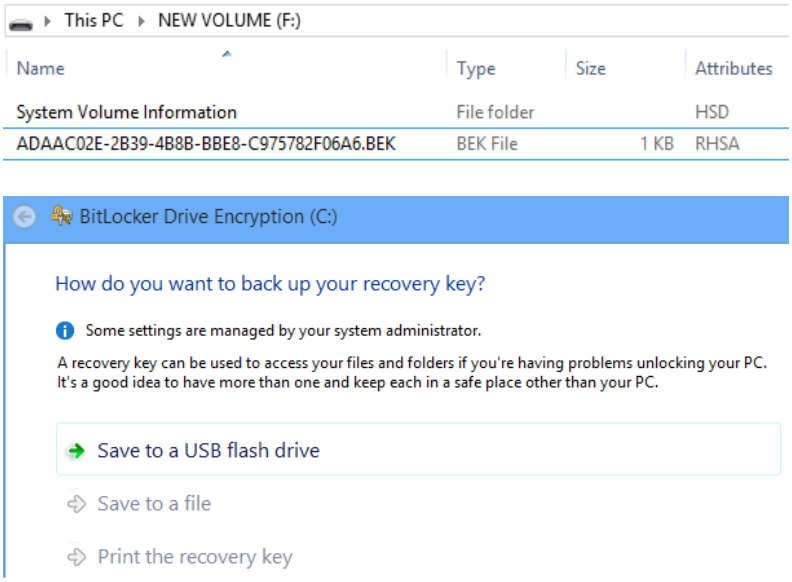
3.5.2 Metódy obnovy kľúča

V prípade, že sa z nejakého dôvodu nedá získať VMK kľúč, je pri štarte systému požadovaný kľúč na obnovu (Recovery Key). Ak používateľ kľúč nezadá, nebude schopný sa dostať k dátam uloženým na šifrovanom disku. Tento kľúč je vygenerovaný pri inicializácii Bitlocker šifrovania a môže byť uchovávaný v niekoľkých základných formách.

- **Heslo na obnovu –** 48 číslic rozdelených do ôsmich blokov. Toto heslo môže byť uložené do súboru, vytlačené, príp. uložené v MBAM databáze, v databáze Adresárových Služieb (Active Directory), alebo na Microsoft OneDrive úložisku [26].

Obr. 12: Žiadosť o zadanie hesla na obnovu [26].

- **USB kľúč so súborom na obnovu (Recovery USB Key)** – súbor s kľúčom je uložený na prenosnom pamäťovom médiu. Súbor má veľkosť 1 KB a jeho názov sa nemôže modifikovať. Médium na ktorom sa kľúč nachádza, musí byť počas obnovy pripojené [26].

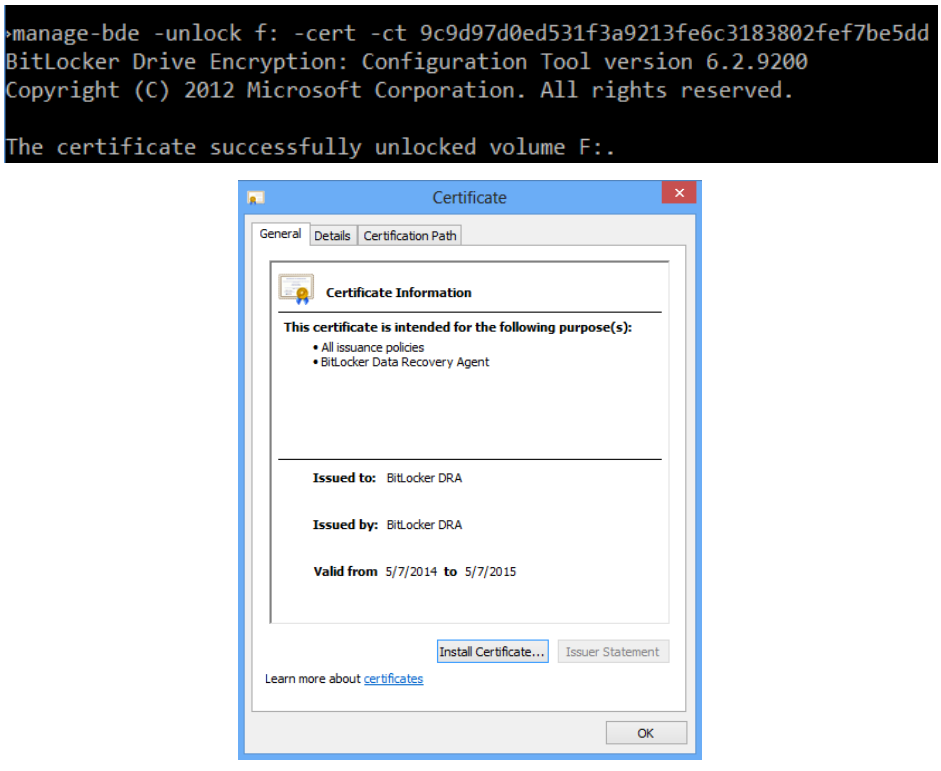


Obr. 13: Heslo na obnovu – USB kľúč [26].

- **Heslo na obnovu uložené prostredníctvom Microsoft konta** – heslo nie je viditeľné medzi štandardnými OneDrive dokumentami, ale je potrebné ísť do „recoverykey“ kontajneru: **https://onedrive.live.com/recoverykey** [26].

Obr. 14: Heslo na obnovu – Microsoft konto [26].

- **Agent na obnovu dát (Data recovery Agent - DRA) –** DRA certifikát môže byť vygenerovaný pre každý novo-zašifrovaný disk. Konfiguračné nastavenia sa nachádzajú v doménových skupinových politikách: Computer Configuration\Windows Settings\Security Settings\Public Key Policies\Bitlocker Drive Encryption [26].



Obr. 15: Agent na obnovu dát [26].

3.5.3 **Zabezpečenie procesu zavádzania**

Systém Windows 10 obsahuje viacero úrovní ochrany pred škodlivým kódom. Aplikácie ako Windows Defender, ktorý sa používa na detekciu škodlivých aplikácií, alebo technológia SmartScreen filter, ktorá upozorňuje používateľov, pri spustení nedôveryhodnej aplikácie, sú však typom ochrany, ktorá chráni systém až po jeho spustení [29].

Moderný malware je pritom schopný časť svojho kódu nainštalovať do oblastí, ktoré sú pred očami bežného užívateľa skryté a načítavajú sa ešte pred samotným spustením operačného systému. Týmto sú schopné vyššie uvedené nástroje obísť a narušiť tak bezpečnosť operačného systému [29].

Pri spustení počítača s operačným systémom Windows 10, príp. s iným systémom podporujúcim UEFI rozhranie, funkcia Trusted Boot chráni systém pred škodlivým softvérom od okamihu, keď je systém zapnutý, až pokiaľ sa pod samotným operačným systémom nenaštartuje antivírusový program. V prípade, že sa škodlivému kódu podarí do systému preniknúť, Trusted Boot pomocou zabudovaných procesov na kontrolu integrity tento prienik spoľahlivo deteguje [29].

„Windows 10 podporuje štyri funkcie, ktoré zabraňujú načítaniu rootkitov[1] a bootkitov[2] počas procesu spúšťania:

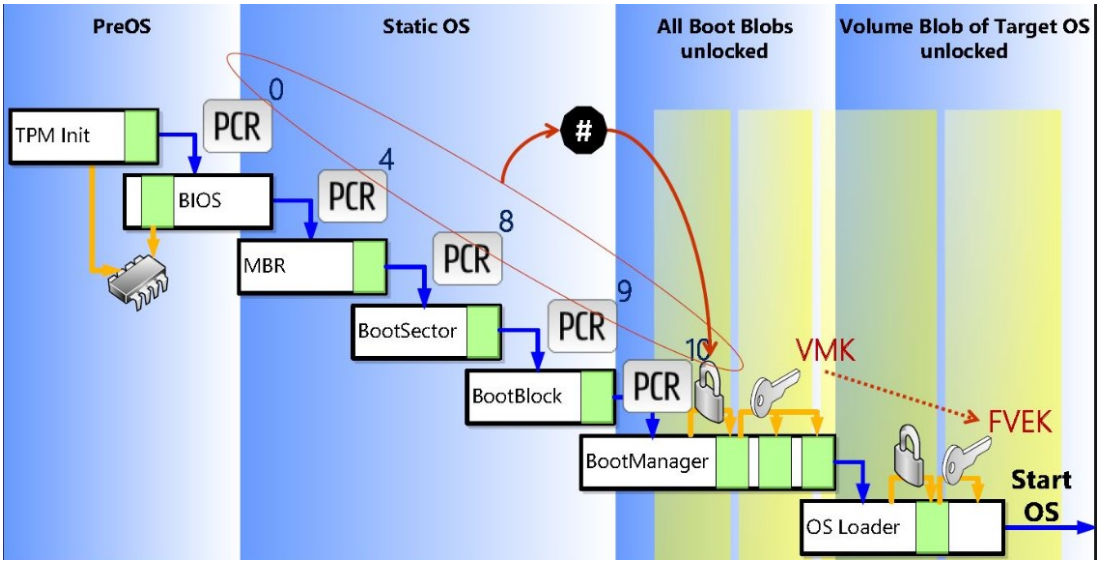
- ***Secure Boot -** počítače s UEFI rozhraním a TPM modulom, možno konfigurovať tak, aby načítavali iba dôveryhodné zavádzače operačných systémov.*
- ***Trusted Boot** - systém Windows pred načítaním skontroluje integritu každého komponentu procesu spustenia.*
- ***Early Launch Anti-Malware (ELAM) -** ELAM testuje všetky ovládače skôr, ako sa načítajú a tým zabraňuje načítaniu neschválených ovládačov.*
- ***Measure Boot** - firmvér počítača zapíše do denníka celý proces zavádzania a systém Windows ho môže následne odoslať na dôveryhodný server, ktorý dokáže objektívne vyhodnotiť stav tohto počítača“ [29].*

[1]Rootkit – *„súbor počítačových programov, pomocou ktorých je možné maskovať prítomnosť škodlivého kódu v systéme“ [30].*

[2]Bootkit – množina počítačových programov, ktoré umožňujú zmeniť, alebo nahradiť zavádzač operačného systému tak, aby sa pri jeho načítavaní súčasne spúšťal aj škodlivý kód.

3.5.4 Zavádzací proces počítača s TPM čipom a so zapnutým Bitlocker šifrovaním

V rámci počiatočnej fázy zavádzania systému, sa kontroluje jeho integrita a zároveň sa zapisujú hodnoty sledovaných oblastí do PCR registrov TPM čipu (tieto registre sú kontrolované a údaje do nich zapisované v priebehu celého zavádzacieho procesu). Následne sa hľadajú jednotlivé obnovovacie kľúče (najprv sa zisťuje prítomnosť CLEAR a v ďalšom kroku prítomnosť kľúča na obnovu). Ak sa v niektorej z týchto fáz vyskytne problém, užívateľ je vyzvaný, aby zadal Bitlocker heslo na obnovu (48-bitové číslo). Ak sa žiadny problém nevyskytol a používa sa dodatočné overovanie, musí užívateľ zadať PIN, alebo vložiť USB disk, príp. sa spustí proces získavania kľúča pomocou Network Unlock funkcie. Po úspešnom získaní kľúča sa opätovne kontrolujú hodnoty v PCR registroch TPM čipu. Ak sú všetky hodnoty v poriadku, potom je TPM požiadaný o vydanie VMK kľúča. V ďalšom kroku sa pomocou digitálneho podpisu (MAC[3] - Message authenticity Check), ktorý bol vytvorený s využitím VMK, kontroluje zavádzač operačného systému (winload.exe). Finálne, po úspešnej kontrole integrity je uvoľnený VMK kľúč použitý na dešifrovanie FVEK a začína sa proces zavádzania operačného systému Windows [27].



Obr. 16: Zavádzací proces počítača s Bitlocker šifrovaním a TPM [31].

[3]MAC – skratka MAC v tomto prípade neznamená „Media Access Control“ adresa, ktorú poznáme zo segmentu počítačových sietí, ale predstavuje výraz „Message Authenticity Check“, tzv. kontrolu dôveryhodnosti správy v procese zavádzania systému pri použití Bitlocker nástroja.

3.6 Možnosti centrálnej správy

3.6.1 Microsoft BitLocker administrácia a manažment (MBAM)

je nástroj, ktorý je súčasťou Microsoft desktop optimalizačného balíčka (MDOP). MDOP je portfólio technológií, dostupných ako predplatné pre zákazníkov s platnou „Software Assurance“ službou.

MBAM poskytuje zjednodušené administratívne rozhranie pre Bitlocker šifrovanie jednotiek a poskytuje nasledovné rozšírené možnosti:

- Umožňuje správcom systému automatizovať proces šifrovania zväzkov na klientských počítačoch v rámci celej organizácie.
- Vynucuje centrálne nastavenia Bitlocker šifrovacích politík, ktoré boli definované v rámci organizácie.
- Umožňuje bezpečnostným správcom rýchlo určiť, či sú jednotlivé počítače, alebo skupiny počítačov v zhode s definovanou firemnou politikou.
- V kombinácii s Microsoft System Center Configuration Manager (SCCM), poskytuje centralizované spravovanie reportov a správu hardvéru.
- Umožňuje koncovým používateľom svojpomocne si obnoviť prístup k zašifrovanému disku, pomocou funkcií Samoobslužného portálu - keď používateľ zabudol svoj PIN, heslo, alebo keď sa zmenili BIOS nastavenia.
- Umožňuje bezpečnostným administrátorom, ľahko kontrolovať žiadosti o prístup ku obnovovacím kľúčom [32].

Požiadavky:

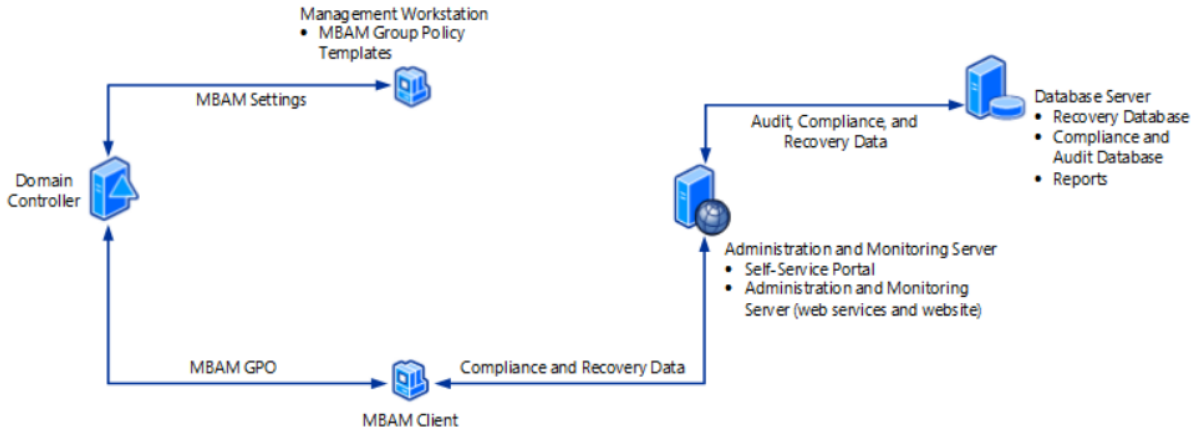
Server

- Požadované MBAM role a účty – užívatelia a skupiny vytvorené prostredníctvom Adresárových služieb (AD DS).
- Podporovaná verzia operačného systému – Windows server 2008 R2 až Windows Server 2019 (Štandard, Enterprise, alebo Datacenter).
- Databáza – podporovaná verzia SQL (2008 R2 až 2017, Štandard, Enterprise, alebo Datacenter) a nevyhnutné SQL oprávnenia.
- Windows PowerShell 3.0 a novší.

- Samoobslužný Portál (Self-Service Portal)
  - ASP.NET MVC 4.0.
  - SPN – Service Principal Name.
- Administračný a monitoring server
  - Web server rola a požadované doplnky.
  - SSL certifikáty.
  - .NET Framework 4.5.
- Manažment stanica s MBAM doménovými skupinovými šablónami [33].

Klient

- Operačný systém – minimálne Windows 7, edícia Enterprise, príp. Ultimate.
- Klient musí byť členom domény, ktorá je rovnaká, ako doména MBAM serverov, alebo musia mať domény medzi sebou vytvorený požadovaný stav dôvery.
- Nainštalovaný MBAM klientský softvér.
- Nakonfigurované a aplikované doménové skupinové politiky.
- Pevný disk počítača musí mať aspoň dva oddiely a musí byť naformátovaný systémom súborov NTFS.
- TPM čip musí byť povolený v BIOSa a musí byť možné ho resetovať z operačného systému [34].



Obr. 17: MBAM architektúra – “Stand-alone” [35].

3.7 Network Unlock

„Je novou, zaujímavou funkcionalitou implementovanou v systémoch Microsoft Windows 7 a novších. Funkcia zjednodušuje použitie tzv. viacnásobnej (multifaktor) ochrany pri Bitlocker šifrovaní. Informácie potrebné k dešifrovaniu obsahu disku sú uložené v TPM čipe, ale zároveň je systém pri svojom štarte chránený aj PIN kódom, ktorý si užívateľ zvolil, keď povolil šifrovanie daného disku. Pri štarte sa zariadenie automaticky snaží kontaktovať server, na ktorom sú nainštalované Network Unlock komponenty. Ak sa spojenie podarí nadviazať, zariadenia si navzájom vymenia potrebné informácie a užívateľ nemusí zadávať PIN pri štarte systému. V opačnom prípade (server je nedostupný, alebo je klient mimo korporátnej siete), musí užívateľ pri štarte systému zadať definovaný PIN kód“ [36].

Požiadavky pre Network Unlock

Infraštruktúra a servery:

- Operačný systém, minimálne Windows Server 2012 s UEFI inštaláciou a podporou UEFI DHCP ovládačov.
- Systém by mal byt v natívnom móde s vypnutou funkciou CSM (Compatibility Support Module).
- Nainštalované nasledovné komponenty a role Windows Server:
  - BitLocker Network Unlock server funkcionalita.
  - Windows WDS (Windows Deployment Services) rola.
  - DHCP server rola, oddelená od WDS Server role.
- Korektne nakonfigurovaná PKI infraštruktúra.
- Nakonfigurované Network Unlock doménové skupinové politiky [26, 37].

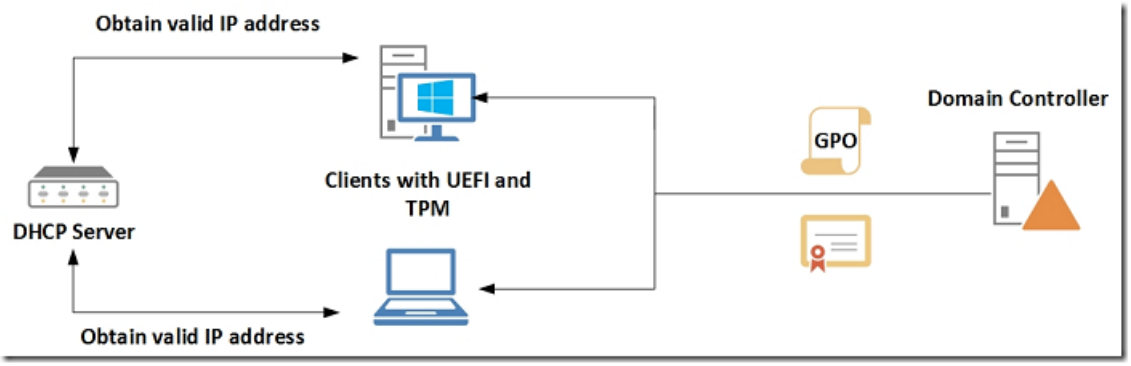
Klient

- Operačný systém Windows 8 a novší, s podporou UEFI špecifikácie 2.3.1.
- Klient musí mať povolený a aktivovaný TPM čip.
- Drôtový, alebo bezdrôtový sieťový adaptér s podporou PXE protokolu [37].

Celý proces odomykania systémového disku pri použití funkcie Network Unlock, môžeme rozdeliť do troch základných fáz:

Fáza 1

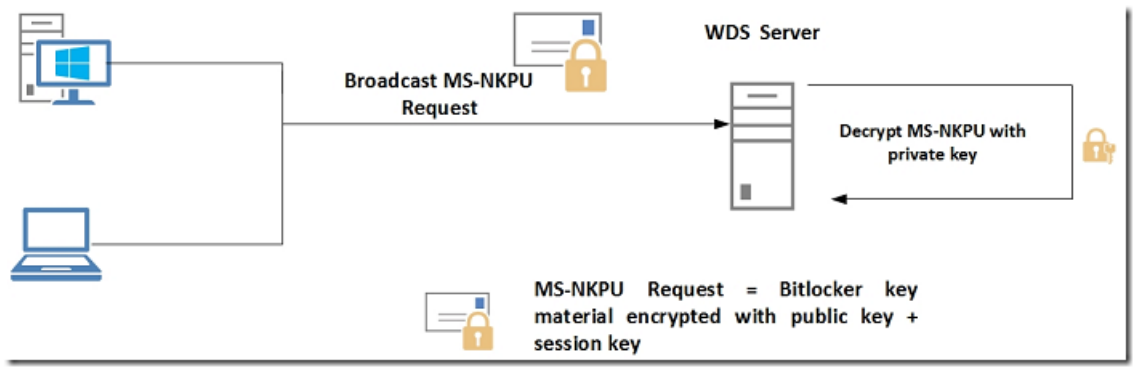
V prvej fáze sa klient, ktorý spĺňa všetky požiadavky a bol skupinovými politikami nakonfigurovaný, aby využíval Network Unlock, snaží pri štarte (ešte pred štartom samotného operačného systému) s použitím UEFI získať IP nastavenia z DHCP servera. Zároveň sa predpokladá, že na klientskom zariadení sa už nachádza potrebný certifikát, ktorý bude v ďalšej fáze využitý na šifrovanie správ [37].



Obr. 18: Network Unlock – Fáza 1 [37].

Fáza 2

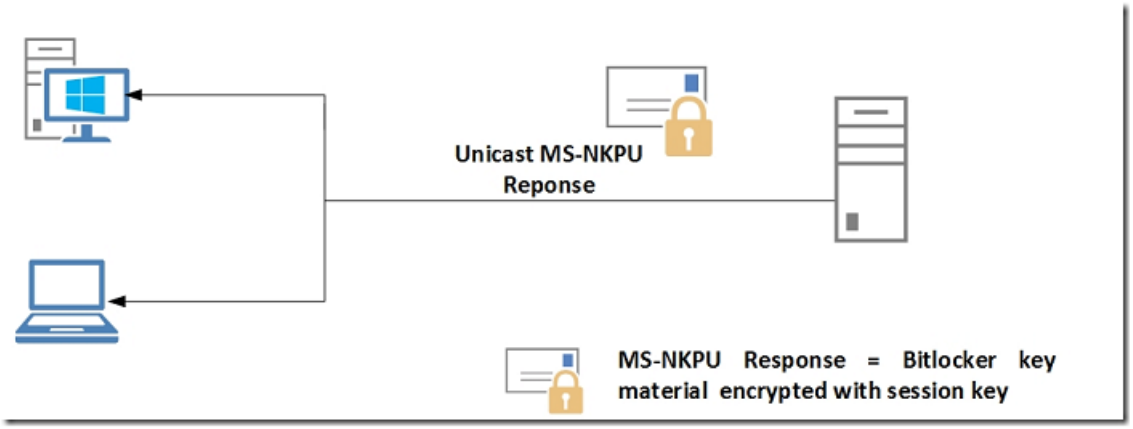
Klient využíva vysielanie špeciálne modifikovaného sieťového paketu, ktorý je zabalený v DHCPinform pakete. Tento obsahuje Bitlocker kľúč, zašifrovaný verejným kľúčom WDS certifikátu a 256 bit kľúč relácie, ktorý sa neskôr použije na ochranu pri následnej komunikácii [37].



Obr. 19: Network Unlock – Fáza 2 [37].

Fáza 3

Potom, čo Network Unlock server príjme požiadavku, dešifruje ju zodpovedajúcim súkromným kľúčom WDS certifikátu a následne zašle späť Bitlocker kľúč, zašifrovaný kľúčom relácie vygenerovaným v predošlej fáze. Po prijatí paketu klient dešifruje Bitlocker kľúč a tak je schopný odomknúť kryptovaný pevný disk a začať proces štartu samotného operačného systému [37].



Obr. 20: Network Unlock – Fáza 3 [37].

„Network Unlock stále využíva TPM na kontrolu integrity platformy. To znamená, že ak sa zmenia hodnoty v PCR registroch (napríklad z dôvodu aktualizácie systému BIOS, výmeny základnej dosky, alebo z dôvodu výskytu škodlivého kódu v zavádzacích komponentoch), bude užívateľ opätovne vyzvaný, k zadaniu kľúča na obnovenie systému Bitlocker. Zadanie tohto kľúča nemôže byť žiadnym spôsobom automatizované.

V niektorých UEFI implementáciách je možné zakázať DHCP verzie 6 priamo z užívateľského rozhrania. Ak sa chce správca uistiť, že Network Unlock využíva IP verzie 4, musí vypnúť IP verzie 6 na sieťovom adaptéry WDS servera. Zavádzací kód na klientskom systéme, sa najprv pokúša komunikovať cez DHCP verzie 6 a až následne, ak je táto komunikácia neúspešná, sa prepne na DHCP verzie 4“ [37].

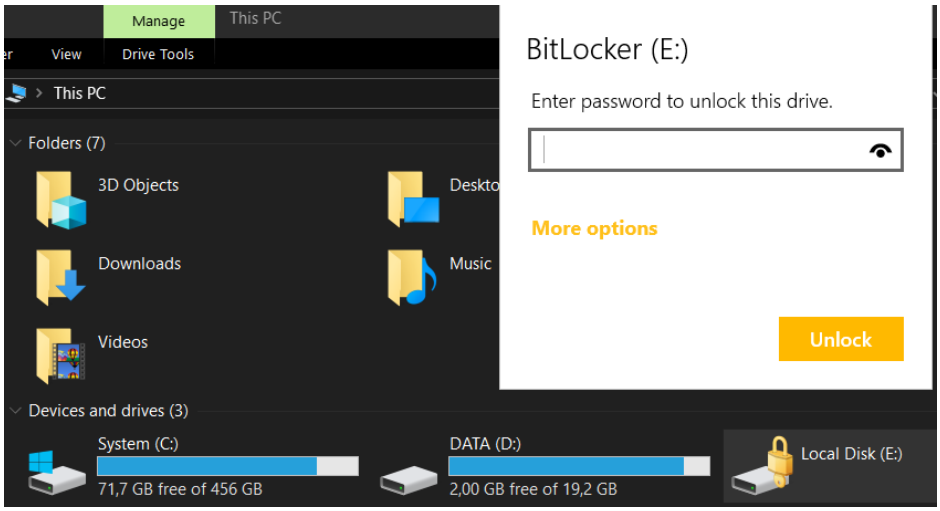
4 BITLOCKER TO GO

„Je verziou Bitlocker aplikácie, určenou primárne na zabezpečenie prenosných a flash USB diskov. Uložené dáta sú šifrované heslom a správca si môže zvoliť, či povolí užívateľom aby si šifrovanie riadili sami, alebo bude pravidlá určovať organizácia centrálne, pomocou doménových skupinových politík“ [36].

Pri šifrovaní pomocou BitLocker To Go sa jedná o šifrovanie celého diskového oddielu (tzv. Full Volume Encryption). Súborový systém musí byť naformátovaný ako NTFS, FAT16, FAT32, alebo exFAT a musí mať minimálne 64MB voľného miesta [38].

Šifrované médium môže byť odomknuté pomocou hesla, alebo s využitím smart karty [38].

„Zväzky zašifrované pomocou nástroja BitLocker To Go majú tzv. hybridný šifrovaný zväzok, čo znamená, že jeden diskový oddiel je nešifrovaný a obsahuje aplikáciu na odomknutie druhého, šifrovaného diskového oddielu. Nešifrovaná časť obsahuje nástroj “BitLocker To Go Reader“, ktorý umožňuje čítanie šifrovaných oddielov v systémoch Microsoft Windows, ktoré nemajú vstavanú podporu Bitlocker nástroja” [39].



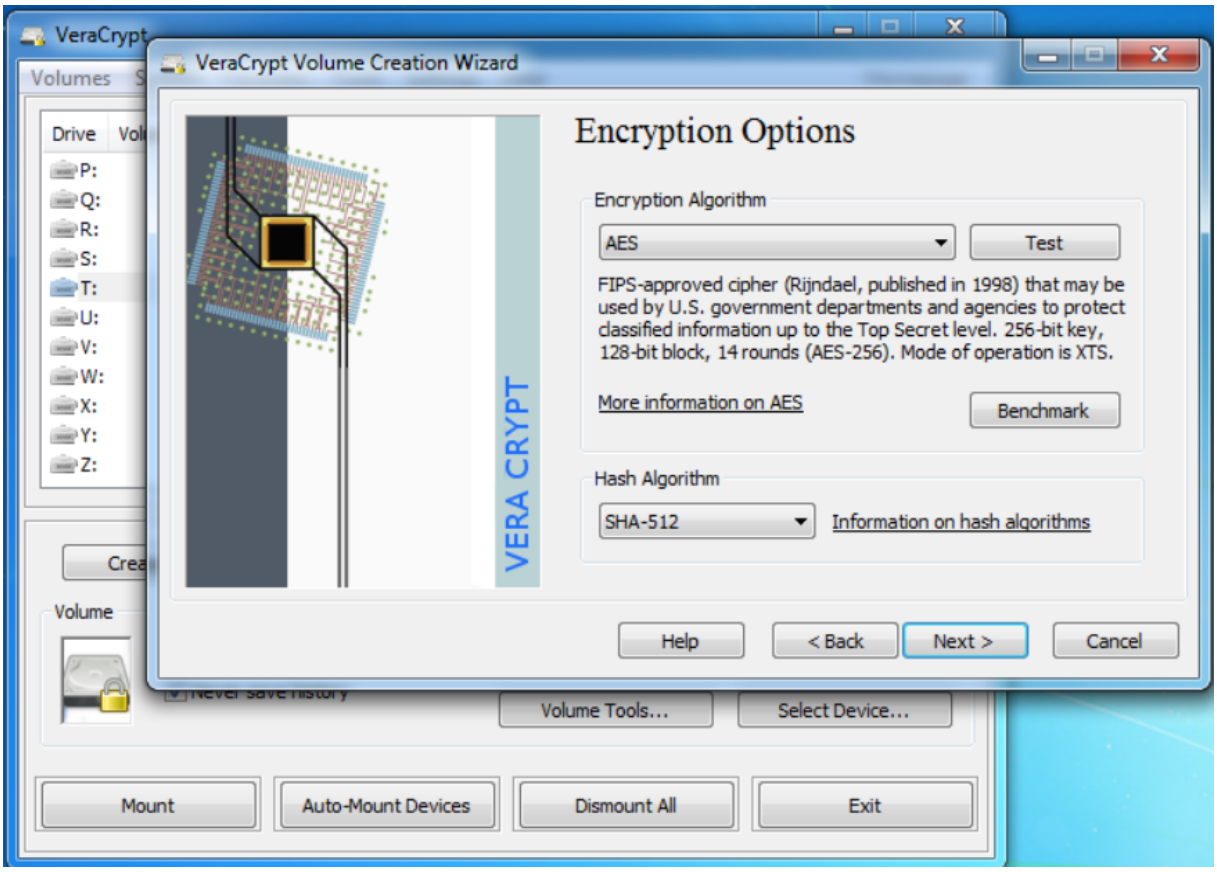

```
Volume E: [Smallie-4T]
[Data Volume]

    Size:                 3725.99 GB
    BitLocker Version:    2.0
    Conversion Status:    Fully Encrypted
    Percentage Encrypted: 100.0%
    Encryption Method:    AES 128
    Protection Status:    Protection On
    Lock Status:          Unlocked
    Identification Field: Unknown
    Automatic Unlock:     Disabled
    Key Protectors:
        Password
        Numerical Password
```

Obr. 21: Bitlocker To Go, vlastný zdroj.

5 SOFTVÉROVÉ NÁSTROJE NA ŠIFROVANIE DISKOV

5.1 VeraCrypt

VeraCrypt je voľne dostupný šifrovací nástroj určený pre operačné systémy Windows, Linux a Mac OSX.



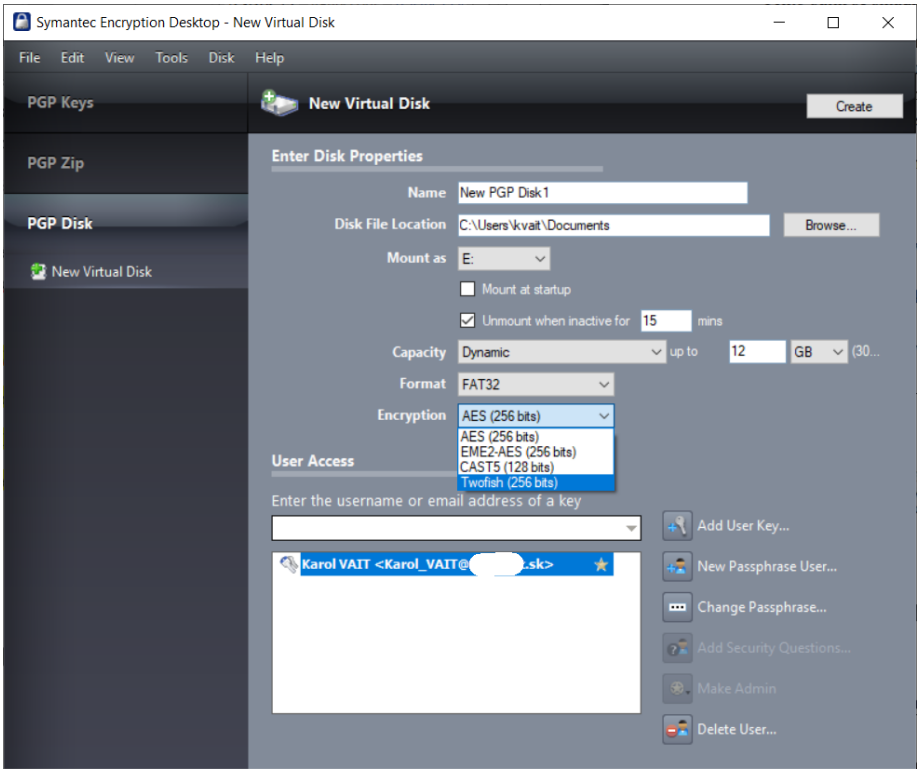
Obr. 22: VeraCrypt [40].

Veracrypt je nástupcom populárneho programu TrueCrypt, ktorého vývoj bol ukončený. Tento nástroj je založený na zdrojovom kóde TrueCrypt-u, pričom pribudli mnohé vylepšenia. S pohľadu bezpečnosti medzi najzaujímavejšie patria:

- **Šifrovaný systémový oddiel** – 327 661 iterácií pri použití PBKDF2-RIPEMD160 algoritmu vo VeraCrypt, oproti 1 000 iteráciám používaných u Truecrypt-u.
- **Štandardné kontajnery a iné oddiely** – 655 331 iterácií pri RIPEMD160 (resp. 500 000 iterácií pri SHA-2 a Whirpool) u VeraCrypt-u, oproti maximálne 2 000 iteráciám využívaným v TrueCrypt-e [7, 40].

5.2 Symantec Encryption Desktop

Je založený na štandarde PGP a obsahuje balík šifrovacích nástrojov, ktorý poskytuje komplexné zabezpečenie pre počítačové systémy. Princípom je využitie kľúčového páru: verejný a privátny kľúč. Privátny kľúč a k nemu prislúchajúca, užívateľom definovaná fráza, sa vytvára pri inštalácii aplikácie. Verejným kľúčom potom odosielateľ šifruje správu – napr. v prípade mailového modulu.



Obr. 23: Symantec Encryption Desktop, vlastný zdroj.

Balík tvoria tieto 3 základné moduly:

- **Symantec Desktop Email** – automaticky šifruje, podpisuje, dešifruje a overuje mailové správy.
- **Symantec File Share Encryption** – umožňuje autorizovaným používateľom zdieľanie chránených súborov.
- **Symantec Drive Encryption** – sa využíva na zašifrovanie celého obsahu pevného, externého, alebo USB disku. Tento modul zároveň navyše umožňuje:
    - Použiť časť priestoru na pevnom disku, ako úložisko pre šifrovaný virtuálny disk
    - Vytvárať chránené ZIP archívy
    - Bezpečné zmazanie súborov a adresárov [15, 41].

5.3 EFS

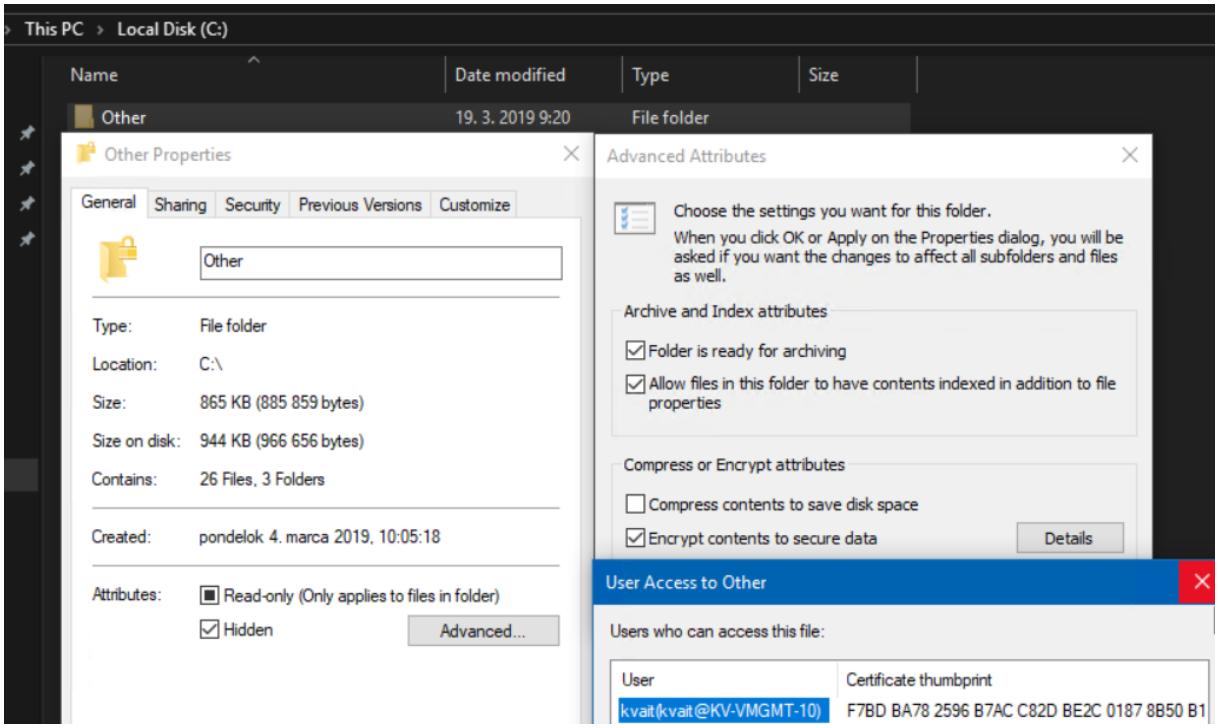
Táto funkcionalita je súčasťou Microsoft Windows operačných systémov.

„EFS chráni citlivé dáta vo všetkých typoch súborov, ktoré sú uložené na súborovom systéme NTFS. Používa symetrický kľúč v kombinácii s technológiou PKI“ [36]. EFS na šifrovanie a dešifrovanie dát využíva jeden z nasledujúcich symetrických šifrovacích algoritmov:

- **3DES a DESX** – staršie protokoly, využívane hlavne v systémoch Windows XP, resp. Windows server 2000.
- **AES 256** – predvolená hodnota v prípade všetkých operačných systémov novších ako Windows XP Service Pack 1 [42].

„Pri EFS, na rozdiel od väčšiny iných externých šifrovacích služieb, šifrovanie súborov nevyžaduje vlastníka súboru na dešifrovanie a opätovné zašifrovanie súboru pri každom použití. Tento proces sa vykonáva automaticky“ [36].

EFS pracuje na odlišnom princípe ako Bitlocker. Šifrované sú iba súbory, uložené do vopred zašifrovaného adresára, alebo dáta, ktoré si užívateľ zašifroval pri ich vytváraní manuálne. Všetky ostatné dáta sú v prípade odcudzenia pevného disku “voľne čitateľné“ potenciálnemu útočníkovi [4].



Obr. 24: EFS, vlastný zdroj.

5.4 Stručné Porovnanie Jednotlivých Produktov

Každý z vyššie uvedených softvérových nástrojov má svoje výhody aj nevýhody. Použitie vo firemnej sieti však kladie na softvér dodatočné požiadavky. Silný šifrovací algoritmus je iba jednou z viacerých. Rovnako dôležitá je cena, poskytované funkcie, možnosť viacfaktorového overovania, jednoduchosť použitia (pre správcu systému, ako aj pre samotného koncového užívateľa), ale hlavne možnosť centrálnej správy. Vo firemnej sieti, kde je veľké množstvo systémov, je nevyhnutné, aby nástroj podporoval možnosť aplikovať správcom definované politiky. Zároveň musí poskytovať spätnú väzbu vo forme grafov, reportov, alebo denníkov udalostí, kde je možné skontrolovať stav ochrany jednotlivých systémov, zariadení a diskov. Otázkou na zamyslenie je aj podpora zo strany výrobcu. V prípade bezplatných programov veľkosť komunity a schopnosti vývojárov reagovať na vzniknuté problémy.

Názov	Šifrovacie algoritmy	Centrálna správa	FDE/FES	Viacfaktorové overovanie	Licencia
Bitlocker	AES (CBC a XTS)	Áno	FDE aj FES	Áno	Súčasť OS[4]
EFS	AES	Nie	FES	Nie	Súčasť OS
Symantec Encryption Desktop	AES, Twofish, Cast5	Áno	FDE aj FES	Áno	Platený
VeraCrypt	AES, Twofish, Camellia, Kuznyechik, Serpent a ich kombinácie	Nie	FDE aj FES	Nie	Bezplatný

Tab. 1: Porovnanie jednotlivých šifrovacích nástrojov, vlastné spracovanie.

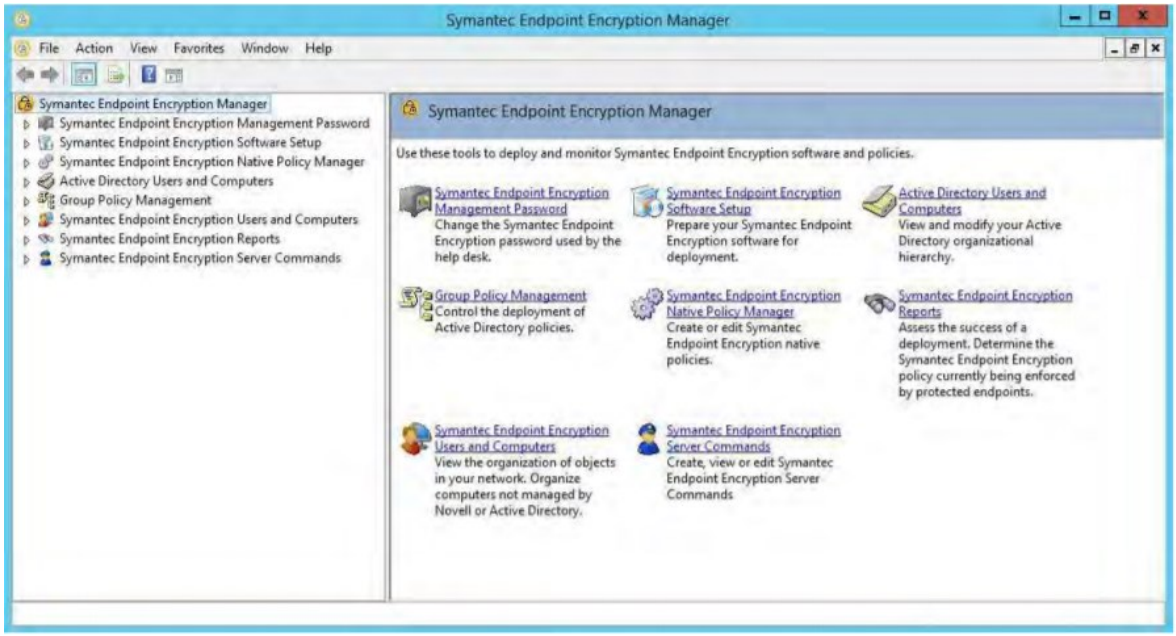
Tabuľka vyššie uvádza množinu vybraných parametrov jednotlivých nástrojov.
Z porovnania je zrejmé, že samotné **EFS** nie je vhodné ako komplexný nástroj na ochranu dát na pevných diskoch. Nepodporuje centralizovanú správu a vyžaduje si „disciplinovaného“ používateľa – šifrujú sa iba dáta uložené do vopred zašifrovaných kontajnerov, príp. dáta, ktoré užívateľ zašifruje manuálne. Situácia sa však značne mení, ak sa EFS skombinuje s Bitlocker šifrovaním.

[4]produkt je súčasťou vybraných edícii Microsoft Windows a v prípade použitia vzdialenej správy (MBAM) je potrebné mať zakúpený podporovaný licenčný program.

Bitlocker podporuje dostatočné množstvo silných šifrovacích algoritmov. Jeho výhodami sú integrácia vo Windows operačnom systéme, možnosť dodatočnej formy overovania a podpora centrálnej správy. Za hlavnú nevýhodu sa považuje uzavretosť kódu, čo zamedzuje jeho revidovaniu širokou internetovou komunitou. Užívateľovi tak neostáva iná možnosť, iba sa spoľahnúť na vyhlásenia spoločnosti Microsoft, že produkt neobsahuje žiadne zadné vrátka, ktoré by mohli narušiť bezpečnosť celého riešenia.

Veracrypt poskytuje najväčšie množstvo šifrovacích algoritmov, s dostatočnou veľkosťou kľúča. Zároveň je produkt bezplatný, čo môže byť v určitých prípadoch výhodou. Veracrypt však nemá možnosť centrálnej správy, čo tento nástroj značne znevýhodňuje pre nasadenie vo firemnej sieti.

Symantec Encryption Desktop, takisto ako Bitlocker, podporuje silné šifrovacie algoritmy, je možné ho centrálne spravovať a povoliť viacfaktorové overovanie. Za nevýhody môžeme považovať náročnejšiu implementáciu viacfaktorového overovania. Samozrejme, produkt nie je možné (okrem 30 dňovej skúšobnej verzie) používať zadarmo.



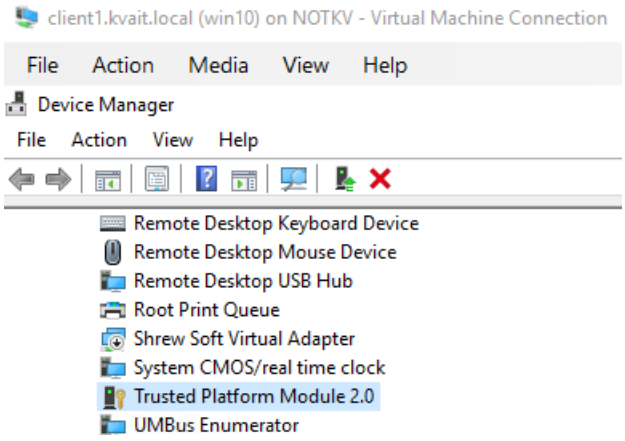
Obr. 25: Symantec Endpoint Encryption Manager [43].

PRAKTICKÁ ČASŤ

6 PRÍKLAD NASADENIE BITLOCKER ŠIFROVANIA

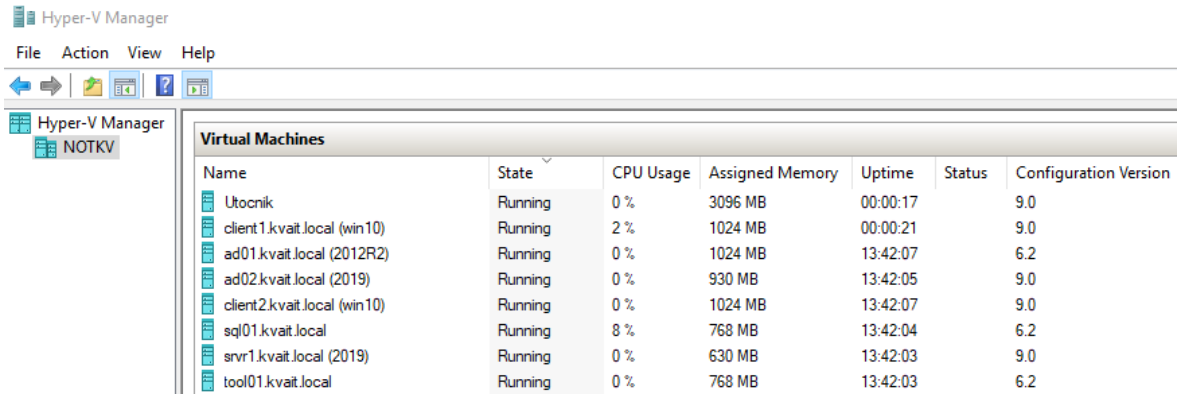
V tejto časti diplomovej práce sa už počíta s tým, že vo virtuálnom prostredí na platforme Microsoft Hyper-V sú nainštalované a nakonfigurované základné prvky infraštruktúry.

Ako virtualizačný „server“ sa využíva Windows 10 Enterprise, verzie 1809 s najnovšími aktualizáciami výrobcu. Fyzická stanica obsahuje TPM modul verzie 2.0. Virtuálne servery a testovacie klientské stanice, majú vo vlastnostiach povolené funkcie Secure Boot a TPM.



Obr. 26: Virtuálny TPM modul, vlastný zdroj.

Ako sieťový adaptér využívajú všetky virtuálne servery a stanice dedikovanú sieť. Všetky ostatné hodnoty, ako poradie zavádzania, integračné služby, ako aj ostatné parametre hardvéru boli ponechané na predefinovaných hodnotách. Veľkosť operačnej pamäte a počet procesorových jadier bol nastavený na najnižšie odporúčané hodnoty.



Obr. 27: Zoznam virtuálnych serverov a staníc, vlastný zdroj.

Vo virtuálnom prostredí boli z dôvodu otestovania Bitlocker scenárov vytvorené dva základné typy systémov.

- **Servery** - virtuálne systémy s operačnými systémom Windows Server 2019 Datacenter, resp. Windows Server 2012 R2 Datacenter. Na serveroch boli nainštalované a nakonfigurované všetky potrebné role a služby. Každý server tak plní špecifickú rolu (alebo role) a je zaradený v doméne.
- **Klientské stanice** – virtuálne počítače s operačným systémom Windows 10 (verzia 1809). Stanice boli použité ako koncoví klienti, na ktorých prebiehalo šifrovanie pevných diskov. Virtuálna stanica s názvom „Utocnik“ nemá nainštalovaný žiadny operačný systém a slúži ako počítač, do ktorého sa pripájali šifrované disky z ostatných klientských staníc.

Tabuľky existujúcich systémov:

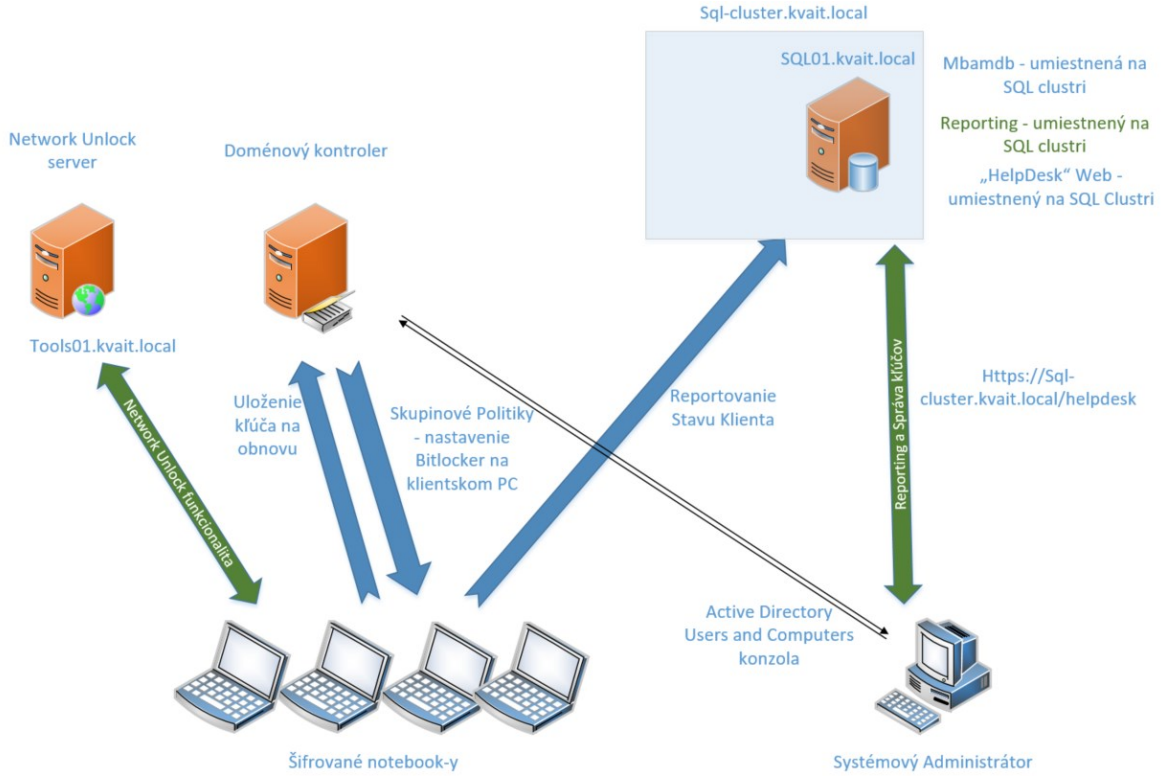
Názov Servera	Operačný Systém	Služby a Role
ad01.kvait.local	Windows Server 2012 R2	Doménový Radič, DNS, DHCP, Certifikačná Autorita
ad02.kvait.local	Windows Server 2019	Doménový Radič, DNS
sql01.kvait.local	Windows Server 2012 R2	SQL Server 2014, SQL Reporting, WEB Server (IIS)
tools01.kvait.local	Windows Server 2012 R2	WDS, Network Unlock

Tab. 2: Existujúce virtuálne servery a ich konfigurácia, vlastné spracovanie.

Názov Klienta	Operačný Systém	Šifrovanie Disku
Client1.kvait.local	Windows 10 (1809)	XTS-AES 128 bit, resp. 256 bit
Client2.kvait.local	Windows 10 (1809)	AES 256 bit
Srv1.kvait.local	Windows Server 2019	žiadne
Utocnik	žiadny	žiadne

Tab. 3: Existujúci klienti a ich konfigurácia, vlastné spracovanie.

6.1 HLAVNÉ KOMPONENTY RIEŠENIA



Obr. 28: Komponenty riešenia, vlastný zdroj.

6.1.1 Adresárové Služby

Doména „kvait.local“ je jedinou doménou v lese. Funkčný level domény, aj samotného lesa, je Windows Server 2012 R2. Všetky operačné role (FSMO) sa nachádzajú na doménovom radiči ad01.kvait.local.

Všetky servery a stanice, boli zaradené do domény a v rámci doménovej organizačnej štruktúry zaradené do požadovanej organizačnej jednotky. Pre potreby testovania, boli vytvorené dve organizačné jednotky, umiestnené priamo v koreňovej časti. Nazvané boli „Bitlocker AES“ a „Bitlocker XTS-AES“. Servery majú manuálne nakonfigurované sieťové nastavenia. Všetky testovacie systémy využívajú na získanie sieťových nastavení DHCP službu a DNS smeruje na doménové radiče - DNS služba je integrovaná v rámci adresárových služieb.

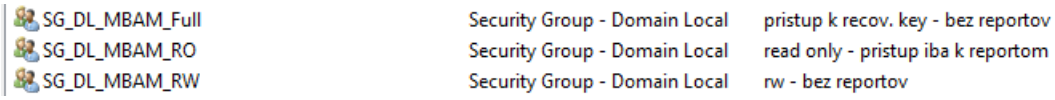
6.1.1.1 BITLOCKER DOMÉNOVÉ POLITIKY A SKUPINY

Pre správnu funkčnosť a možnosť centrálne spravovať šifrované zariadenia boli adresárové služby doplnené o špeciálne šablóny, ktoré umožňujú konfigurovať rozšírené možnosti šifrovania pomocou MBAM („Computer Configuration/Policies/Administrative Templates/Windows Components/MDOP MBAM (Bitlocker Management)“.

Zariadenie, ktoré chceme šifrovať, musí byť pripojené do domény a musia na správne aplikovať doménové politiky. Politika nastavuje parametre špecifické pre daný počítač. Nie je podstatné aký, ani koľko užívateľov bude počítač využívať.

Nové nastavenia, s ktorými Microsoft prichádza v najnovších verziách svojich operačných systémov, aktuálne nie sú v MBAM podporované. V čase písania tejto práce, bolo preto nevyhnutné niektoré konkrétne nastavenia konfigurovať s použitím štandardnej šablóny vo vetve: „Computer Configuration/Policies/Administrative Templates/Windows Components/Bitlocker Drive Encryption“.

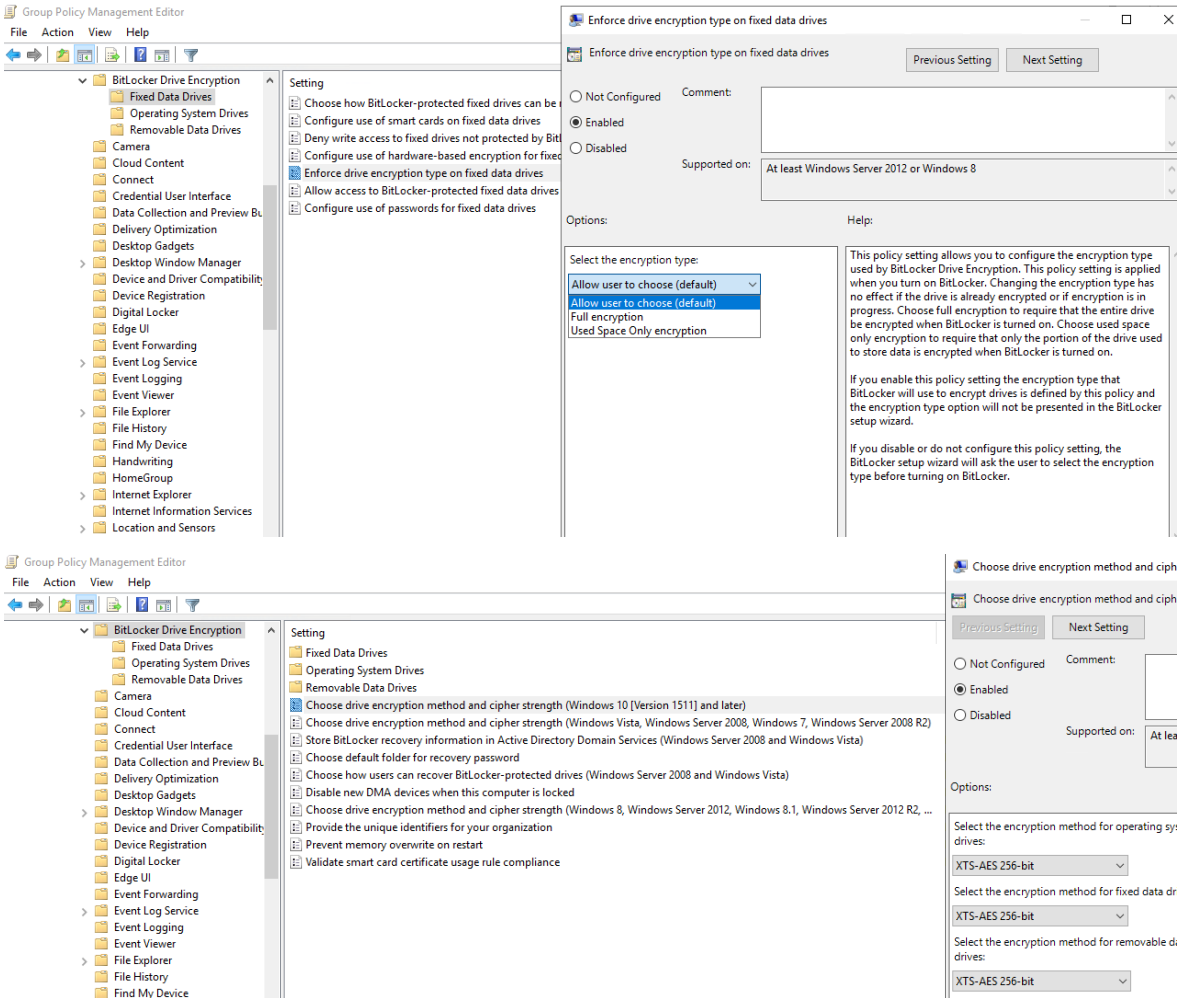
Zároveň boli pre účely správy vytvorené tri nové doménové bezpečnostné skupiny. Administrátor musí byť členom konkrétnej skupiny, aby mohol kontrolovať, alebo spravovať šifrované zariadenia (prezeranie reportov, získanie kľúča, ...).



Obr. 29: Bitlocker doménové skupiny, vlastný zdroj.

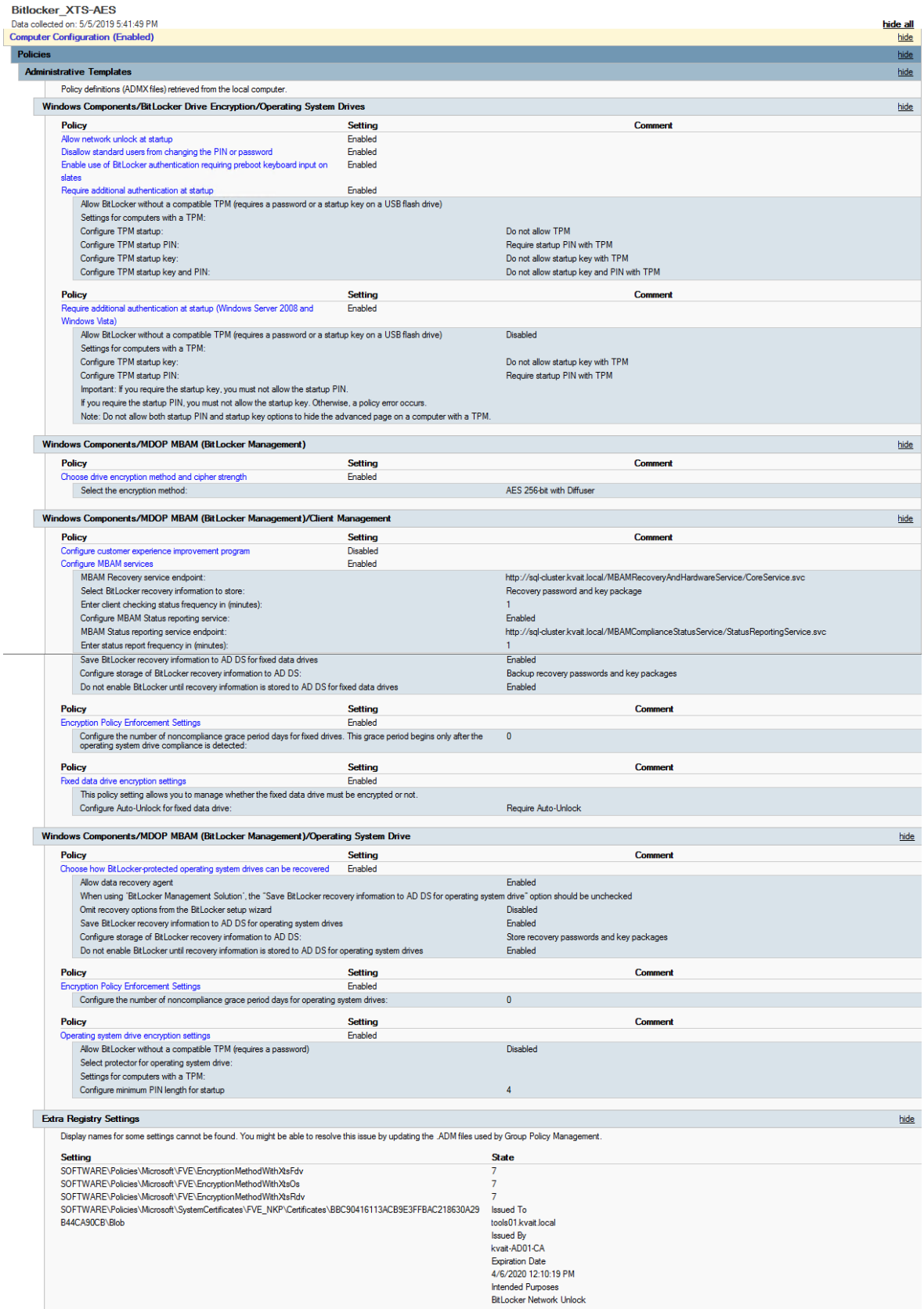
Najdôležitejšie nastavenia Doménových skupinových politík

- **Bitlocker Drive Encryption vetva** – obsahuje dve základné nastavenia, ktoré v tejto chvíli nie sú dostupné v MBAM šablóne. Týmito nastaveniami sú:
  - Enforce Drive Encryption type (Typ šifrovania: Celý disk, alebo iba využité miesto).
  - Drive Encryption Method and Cipher Strenght (Šifrovacie algoritmy pre systémy Windows 10 od verzie 1511: XTS-AES 256, alebo 128 bit).



Obr. 30: Bitlocker – šifrovacie algoritmy a typ šifrovania, vlastný zdroj.

- **MDOP MBAM (Bitlocker Management) vetva** – obsahuje ostatné Bitlocker konfiguračné nastavenia. Medzi najzaujímavejšie patria:
  - Allow Network Unlock at Startup (Povolenie Network Unlock funkcionality).
  - Save Bitlocker Recovery Information to ADDS (Ukladaj Recovery Kľúče do Active Directory).
  - Allow BitLocker Without a Compatible TPM (Počítač musí mať TPM).
  - Configure MBAM services (Adresa MBAM web servera).
  - Configure Minimum PIN length for startup (Minimálny počet znakov v PIN kóde).
  - Extra Registry Settings (Importuje Network Unlock certifikát na klientské stanice).



Bitlocker_XTS-AES

Data collected on: 5/5/2019 5:41:49 PM — hide all

Computer Configuration (Enabled) — hide

Policies — hide

Administrative Templates — hide

Policy definitions (ADMX files) retrieved from the local computer.

Windows Components/BitLocker Drive Encryption/Operating System Drives — hide

Policy	Setting	Comment
Allow network unlock at startup	Enabled	
Disallow standard users from changing the PIN or password	Enabled	
Enable use of BitLocker authentication requiring preboot keyboard input on slates	Enabled	
Require additional authentication at startup	Enabled	
Allow BitLocker without a compatible TPM (requires a password or a startup key on a USB flash drive)		
Settings for computers with a TPM:		
Configure TPM startup:		Do not allow TPM
Configure TPM startup PIN:		Require 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

Policy	Setting	Comment
Require additional authentication at startup (Windows Server 2008 and Windows Vista)	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 key:		Do not allow startup key with TPM
Configure TPM startup PIN:		Require startup PIN with TPM
Important: If you require the startup key, you must not allow the startup PIN.		
If you require the startup PIN, you must not allow the startup key. Otherwise, a policy error occurs.		
Note: Do not allow both startup PIN and startup key options to hide the advanced page on a computer with a TPM.		

Windows Components/MDOP MBAM (BitLocker Management) — hide

Policy	Setting	Comment
Choose drive encryption method and cipher strength	Enabled	
Select the encryption method:		AES 256-bit with Diffuser

Windows Components/MDOP MBAM (BitLocker Management)/Client Management — hide

Policy	Setting	Comment
Configure customer experience improvement program	Disabled	
Configure MBAM services	Enabled	
MBAM Recovery service endpoint:		http://sql-cluster.kvait.local/MBAMRecoveryAndHardwareService/CoreService.svc
Select BitLocker recovery information to store:		Recovery password and key package
Enter client checking status frequency in (minutes):		1
Configure MBAM Status reporting service:		Enabled
MBAM Status reporting service endpoint:		http://sql-cluster.kvait.local/MBAMComplianceStatusService/StatusReportingService.svc
Enter status report frequency in (minutes):		1
Save BitLocker recovery information to AD DS for fixed data drives		Enabled
Configure storage of BitLocker recovery information to AD DS:		Backup recovery passwords and key packages
Do not enable BitLocker until recovery information is stored to AD DS for fixed data drives		Enabled

Policy	Setting	Comment
Encryption Policy Enforcement Settings	Enabled	
Configure the number of noncompliance grace period days for fixed drives. This grace period begins only after the operating system drive compliance is detected:		0

Policy	Setting	Comment
Fixed data drive encryption settings	Enabled	
This policy setting allows you to manage whether the fixed data drive must be encrypted or not.		
Configure Auto-Unlock for fixed data drive:		Require Auto-Unlock

Windows Components/MDOP MBAM (BitLocker Management)/Operating System Drive — hide

Policy	Setting	Comment
Choose how BitLocker-protected operating system drives can be recovered	Enabled	
Allow data recovery agent		Enabled
When using "BitLocker Management Solution", the "Save BitLocker recovery information to AD DS for operating system drive" option should be unchecked		
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		Enabled

Policy	Setting	Comment
Encryption Policy Enforcement Settings	Enabled	
Configure the number of noncompliance grace period days for operating system drives:		0

Policy	Setting	Comment
Operating system drive encryption settings	Enabled	
Allow BitLocker without a compatible TPM (requires a password)		Disabled
Select protector for operating system drive:		
Settings for computers with a TPM:		
Configure minimum PIN length for startup		4

Extra Registry Settings — hide

Display names for some settings cannot be found. You might be able to resolve this issue by updating the .ADM files used by Group Policy Management.

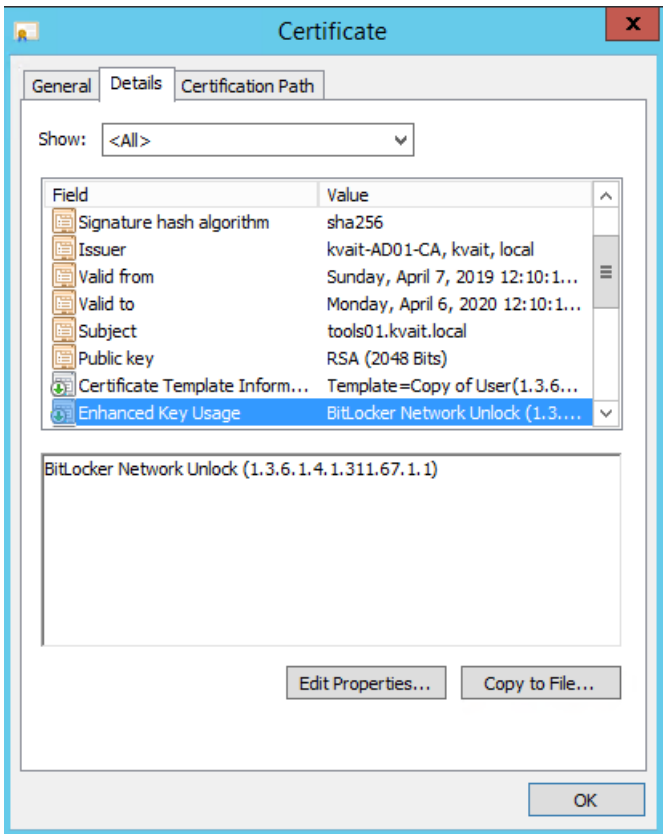
Setting	State
SOFTWARE\Policies\Microsoft\FVE\EncryptionMethodWithXtsFdv	7
SOFTWARE\Policies\Microsoft\FVE\EncryptionMethodWithXtsOs	7
SOFTWARE\Policies\Microsoft\FVE\EncryptionMethodWithXtsRdv	7
SOFTWARE\Policies\Microsoft\SystemCertificates\FVE_NKP\Certificates\BBC90416113ACB9E3FFBAC218630A29B44CA90CB\Blob	Issued To tools01.kvait.local Issued By kvait-AD01-CA Expiration Date 4/6/2020 12:10:19 PM Intended Purposes BitLocker Network Unlock

Obr. 31: Bitlocker skupinové politiky, vlastný zdroj.

6.1.2 Certifikačná autorita

Nevyhnutným predpokladom nasadenia Network Unlock funkcionality je existencia Certifikačnej autority.

Na doménovom radiči ad01.kvait.local bol na základe špeciálne modifikovanej šablóny vygenerovaný certifikát pre Network Unlock. Certifikát bol následne importovaný do certifikačného úložiska na Network Unlock serveri. Distribúcia na klientské stanice je zabezpečená prostredníctvom doménových skupinových politík.

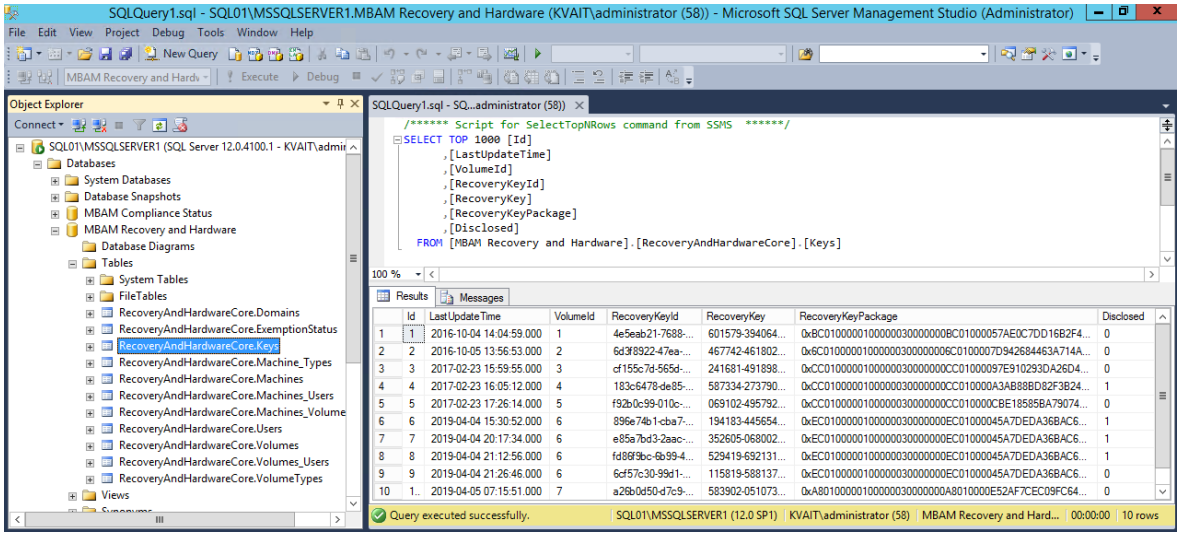


Obr. 32: Bitlocker – Network Unlock certifikát, vlastný zdroj.

6.1.3 DATABÁZA

MBAM databázy, sa nachádzajú na serveri sql01.kvait.local. V databázach sa uchovávajú podrobné informácie o šifrovaných zariadeniach a ich zhode s firemnou politikou. Jedna z databáz je dedikovaná pre reporty. Spomínané databázy sú nazvané nasledovne:

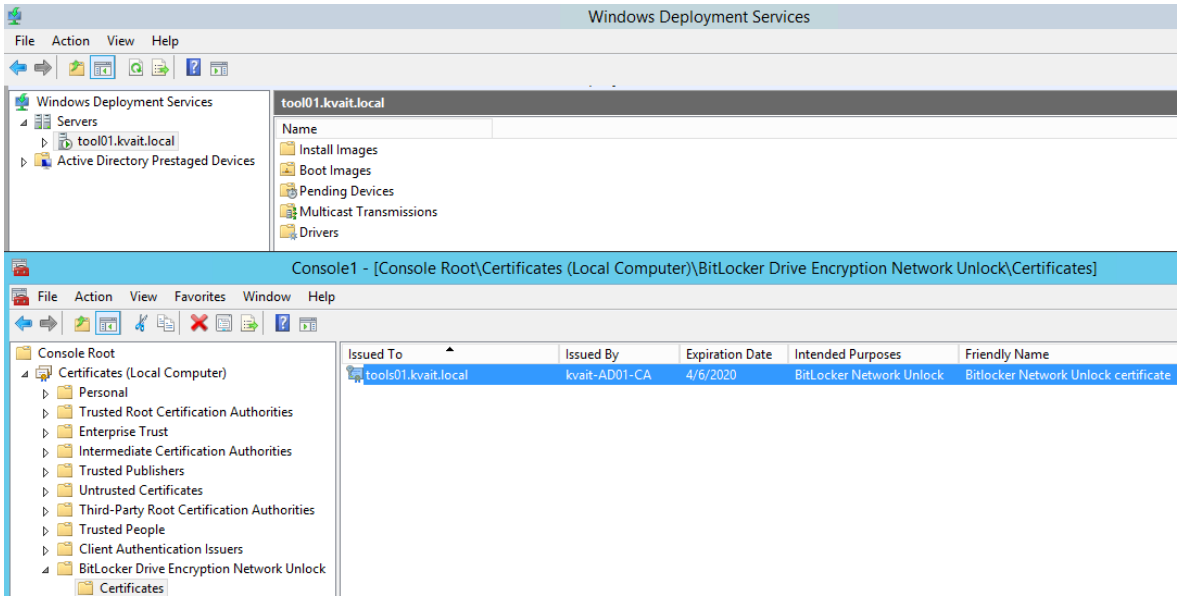
1. MBAM Compliance Status
2. MBAM Recovery and Hardware
3. ReportServer



Obr. 33: Bitlocker – Databáza, vlastný zdroj.

6.1.4 **WDS server**

WDS služba beží na serveri tools01.kvait.local. Službu využíva Network Unlock funkcionalita v momente, keď štartuje klientská stanica pomocou PXE. WDS na serveri nemusí byt reálne nakonfigurovaný, stačí aby bol spustený samotný servis. Zároveň je nevyhnutné, aby na serveri bol na-importovaný korektný certifikát. Ak klient tomuto certifikátu dôveruje, komunikácia medzi klientom a WDS serverom je úspešná a pri štarte klienta nie je potrebné zadávať PIN kód.



Obr. 34: Bitlocker – WDS, vlastný zdroj.

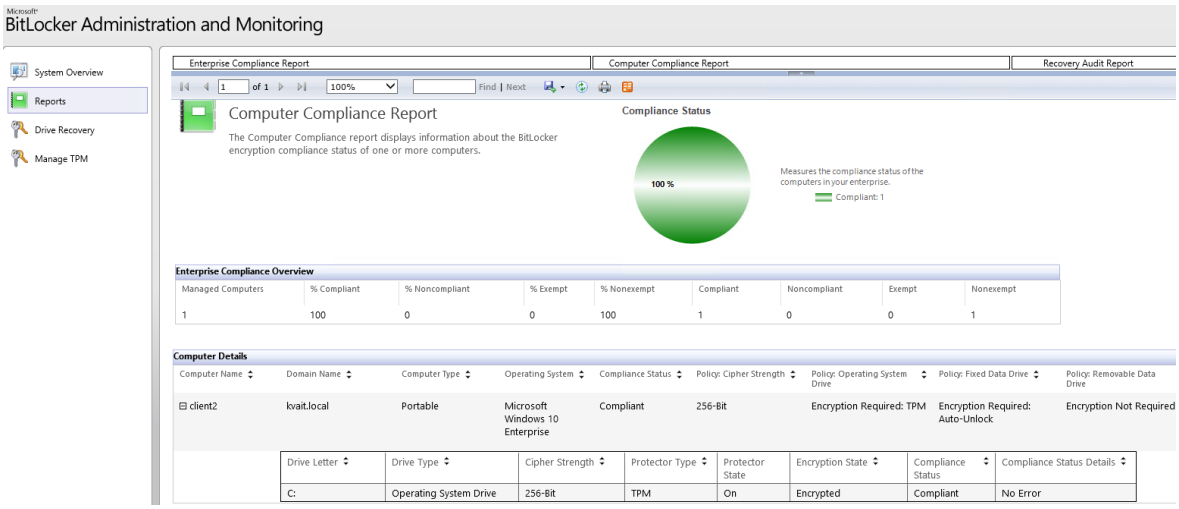
6.1.5 WEB SERVER

WEB server služba bola nainštalovaná na serveri sql01.kvait.local. Základom je rola Internet Information Service (IIS), ktorej úlohou je sprostredkovať spojenie medzi koncovým klientom (šifrované zariadenie), príp. systémovým administrátorom a MBAM databázami. Na tento server zariadenie s povoleným Bitlocker šifrovaním v pravidelných časových intervaloch posiela aktuálne informácie o stave šifrovania. Server zároveň slúži ako hlavný server pre správu Bitlocker nástroja v rámci organizácie.

Webový portál je dostupný na adrese: **https://sql-cluster.kvait.local/helpdesk.**

Jednotlivé časti portálu

- System Overview – popis jednotlivých častí portálu.
- Reports – slúži na generovanie MBAM reportov. Komunikuje s SQL reporting službou na sql01.kvait.local a obsahuje reporty ohľadom šifrovaných zariadení, ich stavu a zoznamy žiadostí o vygenerovanie obnovovacích kľúčov.



Obr. 35: Bitlocker Web server – report, vlastný zdroj.

- Drive Recovery – v tejto časti je schopný správca systému po zadaní potrebných údajov vygenerovať kľúč na obnovu pre konkrétne šifrované zariadenia.
- Manage TPM – spravovanie TPM čipu na šifrovanom zariadení.

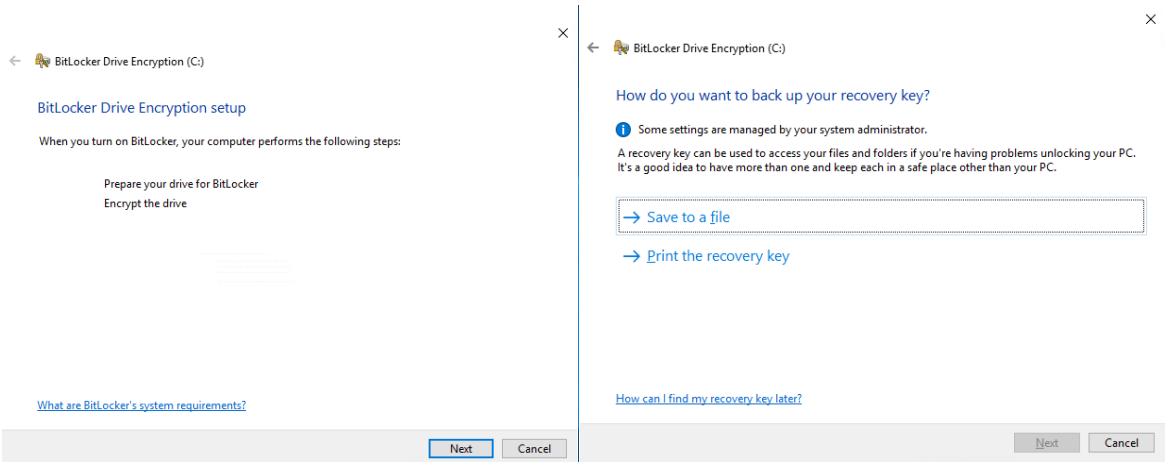
7 VYBRANÉ SCENÁRE NASADENIA

V tejto kapitole budú bližšie popísané štyri vybrané scenáre nasadenia Bitlocker šifrovania. Prvé tri sa budú bližšie zaoberať možnosťami nasadenia na už existujúcu klientskú stanicu. Štvrtý scenár bude riešiť problematiku Bitlocker To Go. Existujú samozrejme aj ďalšie, komplexnejšie spôsoby nasadenia, ako napr. použitie rôznych skriptov, alebo konfigurácia Bitlocker nástroja už pri vytváraní inštalačného média - na inštaláciu koncovej stanice, alebo servera. Z pohľadu jednoduchej demonštrácie sú však tieto komplexné metódy nad rámec cieľov tejto práce.

- **Prvý scenár** popisuje konfiguráciu a správanie klienta, na ktorom bol ešte pred samotným pridaním do domény, alebo pred aplikovaním doménových skupinových politík zapnutý nástroj Bitlocker.
- **Druhý scenár** potom popíše, ako sa správanie Bitlocker nástroja zmení, ak už je počítač pridaný do domény, sú aplikované Bitlocker skupinové politiky a nainštalovaný MBAM klient. V tomto scenári sa počíta s tým, že skupinová politika má nakonfigurovanú podporu viac-faktorového overovania TPM + PIN. Zároveň tento scenár demonštruje funkciu **Network Unlock**.
- **Tretí scenár** nasadenia rieši prípad, keď testovacia stanica je rovnako ako v druhom prípade pridaná do domény, má nainštalovaný balíček s MBAM klientom a aplikované doménové skupinové politiky. Tieto však na rozdiel od vyššie uvedeného scenára (č.2) nevyžadujú dodatočné overovanie prostredníctvom PIN, ale iba šifrovanie s uložením kľúča v TPM module. V tomto prípade sa na rozdiel od obidvoch scenárov uvedených vyššie nepočíta so žiadnym manuálnym zásahom administrátora pri Bitlocker konfigurácii na testovacej stanici.
- **Štvrtý scenár** sa zaoberá použitím nástroja Bitlocker To Go na zašifrovanie prenosných pamäťových médií. Tak ako všetky ostatné scenáre, aj v tomto je možné ovplyvniť výslednú konfiguráciu aplikovaním doménových skupinových politík.

7.1 Scenár č. 1

Testovací počítač (Client1.kvait.local), je síce členom domény, ale doménové politiky, upravujúce Bitlocker konfiguráciu neboli aplikované. Správca systému manuálne povoľuje šifrovanie systémového disku priamo na počítači a je vyzvaný, aby uložil kľúč na obnovu. Systém ponúka možnosť kľúč vytlačiť na tlačiarni, alebo uložiť do súboru. V prípade, že správca zvolí uloženie do súboru, tento nemôže byť uložený na šifrovaný diskový oddiel, alebo disk.



Obr. 36: Scenár č.1 – Kľúč na obnovu, vlastný zdroj.

Ďalšou konfiguračnou voľbou je možnosť zvoliť si „kompatibilný režim šifrovania“, alebo „nový režim šifrovania“. Nový režim štandardne zapína šifrovanie XTS-AES 128 a kompatibilný režim používa AES 128. Najjednoduchšou cestou, ako tieto štandardné nastavenia v doménovom prostredí zmeniť (zmena zo 128 bit na 256 bit), je prostredníctvom doménových skupinových politík[5]. Pre systémy, ktoré v doméne zaradené nie sú, je možné konfigurovať silu šifrovania použitím lokálnych skupinových politík[5], alebo priamo v registroch daného systému.

[5] nastavenia sú rozdelené podľa použitého operačného systému. Windows Vista a Windows 7 umožňujú použiť AES (128, 256 bit) samostatne, alebo s Diffuser. Systémy Windows 8 a 8.1 podporujú AES (128, 256 bit). Najnovšie systémy od Windows 10 verzie 1511, podporujú okrem AES-CBC (128, 256 bit) aj XTS-AES (128 a 256 bit).

Obr. 37: Scenár č.1 – Režim šifrovania, vlastný zdroj.

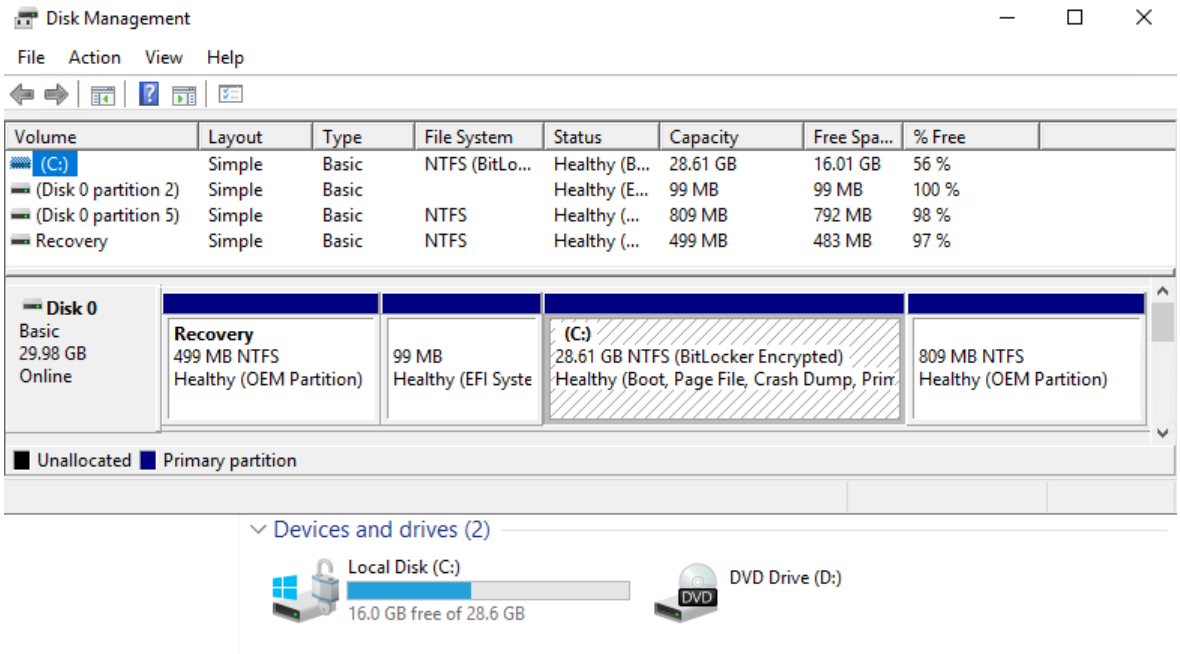
Poslednou možnosťou je voľba typu šifrovania. Správca si aktuálne môže vybrať z dvoch ponúkaných možností:

- **Šifrovanie iba použitého miesta na zvolenej diskovej časti** – je rýchlejšie a vhodné najmä pre nové počítače. Pri tomto type šifrovania si treba uvedomiť, že sú šifrované iba dáta, ktoré sú aktuálne na disku (nie vymazané dáta) a automaticky všetky dáta pridávané v budúcnosti.
- **Šifrovanie celého diskového oddielu** – je síce pomalšie, ale považuje sa za vhodnejšie riešenie v prípade, že sa dané zariadenie už dlhšie používa a na disku by sa mohli nachádzať citlivé údaje v zmazanej forme.

Obr. 38: Scenár č.1 – Typ šifrovania, vlastný zdroj.

Samotné šifrovanie diskového oddielu potom prebieha na pozadí a užívateľ môže ďalej nerušene pracovať.

Po úspešnom zašifrovaní je šifrovaná disková oblasť označená piktogramom kľúčika, prípadne v správcovi diskov ako “Bitlocker encrypted”.



Obr. 39: Scenár č.1 – Výsledok šifrovacieho procesu, vlastný zdroj.

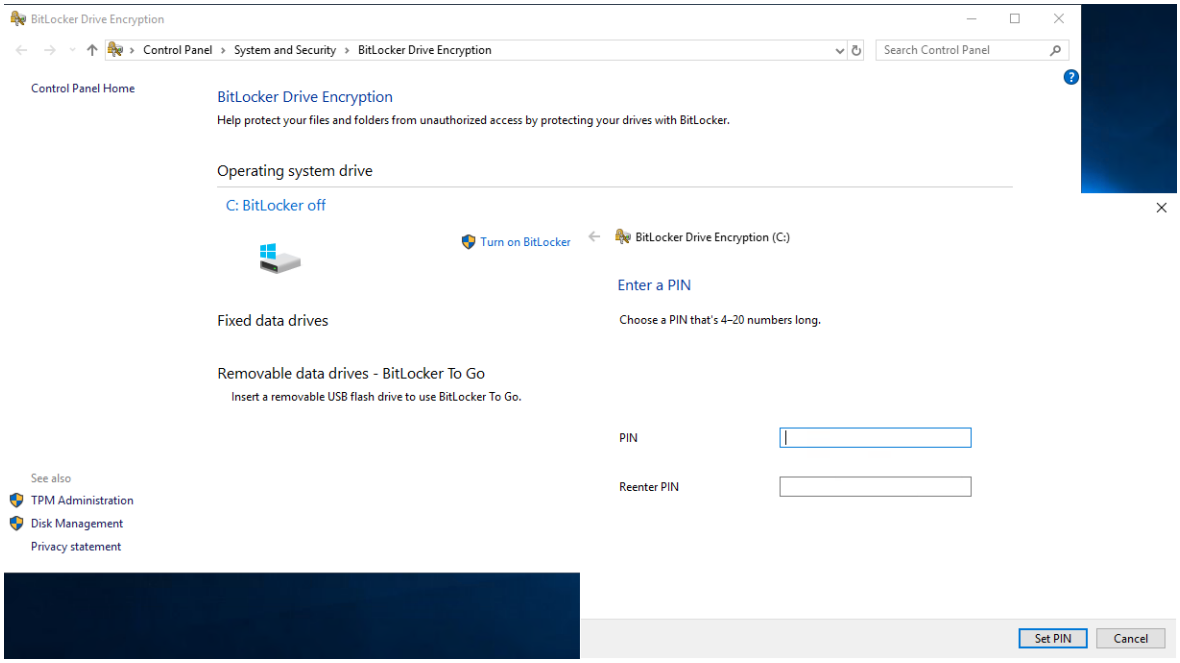
Výsledkom šifrovacieho procesu je disk zašifrovaný s použitím štandardného XTS-AES šifrovacieho algoritmu, s veľkosťou kľúča 128 bit. Šifrované bolo iba použité miesto a využíva sa TPM modul.

```
Volume C: []
[OS Volume]

    Size:                 28.61 GB
    BitLocker Version:    2.0
    Conversion Status:    Used Space Only Encrypted
    Percentage Encrypted: 100.0%
    Encryption Method:    XTS-AES 128
    Protection Status:    Protection On
    Lock Status:          Unlocked
    Identification Field: Unknown
    Key Protectors:
        TPM
        Numerical Password
```

Obr. 40: Scenár č.1 – Výsledok šifrovania, vlastný zdroj.

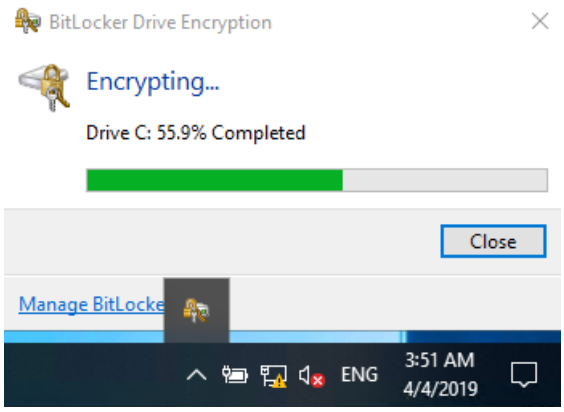
7.2 Scenár č. 2

Testovací počítač (Client1.kvait.local), je členom domény a má nainštalovaný balíček mbamclientsetup.exe. Doménové skupinové politiky, ktoré sa na počítač aplikujú, vynucujú dodatočné overovanie (TPM + PIN) a zároveň umožňujú využitie Network Unlock funkcionality. Správca systému manuálne povoľuje šifrovanie systémového disku priamo na počítači. Ako prvý krok v tomto prípade Bitlocker požaduje zadať PIN kód.



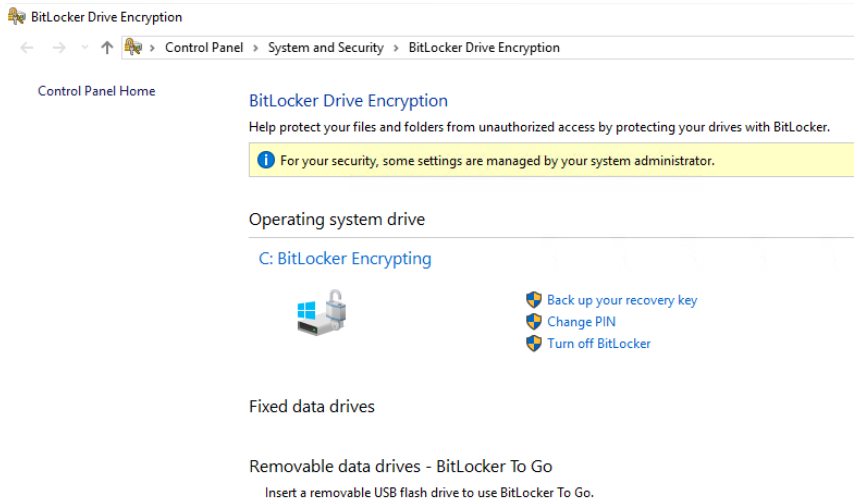
Obr. 41: Scenár č.2 – Zadanie PIN kódu, vlastný zdroj.

Po zadaní PIN kódu je v ďalšom kroku správca vyzvaný na uloženie kľúča na obnovu. Proces samotného šifrovania je potom rovnaký ako v predchádzajúcom scenári. Aktuálny stav je možné sledovať po kliknutí na systémovú lištu.



Obr. 42: Scenár č.2 – Priebeh šifrovania, vlastný zdroj.

Po úspešnom zašifrovaní disku, má užívateľ možnosť zmeniť PIN kód, ktorý mu administrátor nastavil. V prípade, že je nástroj Bitlocker spravovaný prostredníctvom doménových skupinových politík, je táto skutočnosť zobrazená v Bitlocker správcovskej konzole na danom systéme.



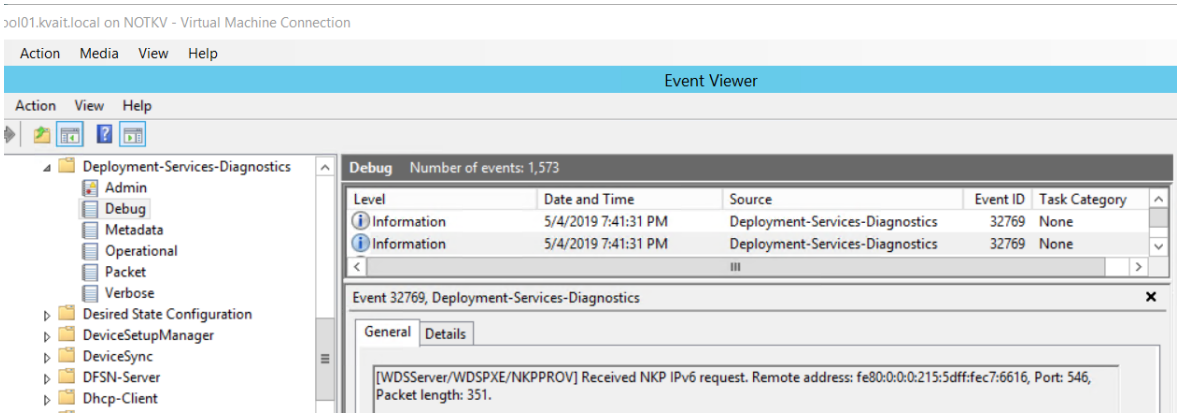
Obr. 43: Scenár č.2 – Možnosť zmeny definovaného PIN kódu, vlastný zdroj.

Výsledkom šifrovacieho procesu je disk šifrovaný pomocou XTS-AES 256 bit šifrovacieho algoritmu, kde je šifrované iba použité miesto a využíva sa TPM aj PIN v kombinácii s Network Unlock.

```
Volume C: []
[OS Volume]

    Size:                 126.40 GB
    BitLocker Version:    2.0
    Conversion Status:    Used Space Only Encrypted
    Percentage Encrypted: 100.0%
    Encryption Method:    XTS-AES 256
    Protection Status:    Protection On
    Lock Status:          Unlocked
    Identification Field: Unknown
    Key Protectors:
        Numerical Password
        TPM And PIN
        Network (Certificate Based)


C:\Users\administrator>
```

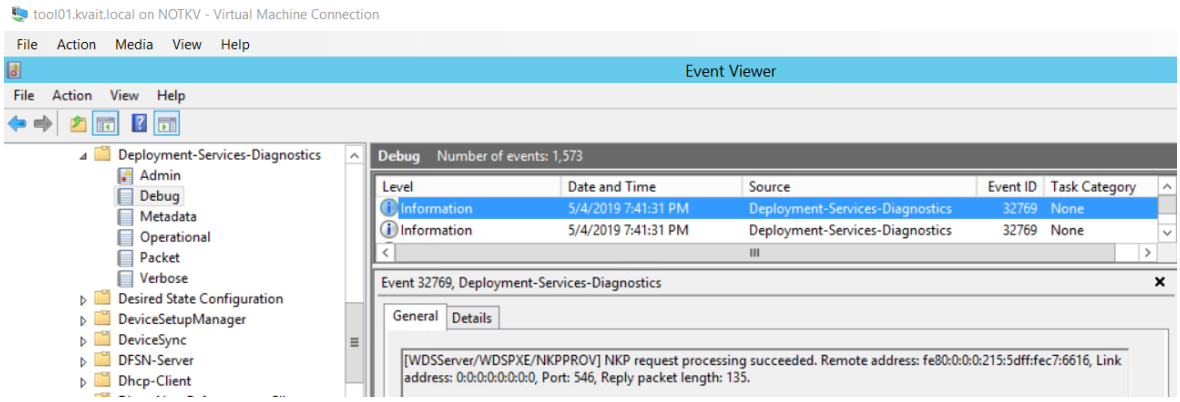
Obr. 44: Scenár č.2 – Výsledok šifrovania, vlastný zdroj.

Pri štarte počítača, je kontaktovaný Network Unlock server. V denníku udalostí na tomto serveri je v časti dedikovanej pre službu WDS záznam, ktorý potvrdzuje prijatie požiadavky z klientskej stanice.



Obr. 45: WDS, prijatie klientskej požiadavky, vlastný zdroj.

Ďalší záznam obsahuje informácie o úspešnom spracovaní klientskej požiadavky a odpovedi na prijatú požiadavku. Po prijatí tejto odpovede klientský počítač automaticky pokračuje v zavádzaní systému. Manuálne zadanie užívateľského PIN kódu nie je potrebné.



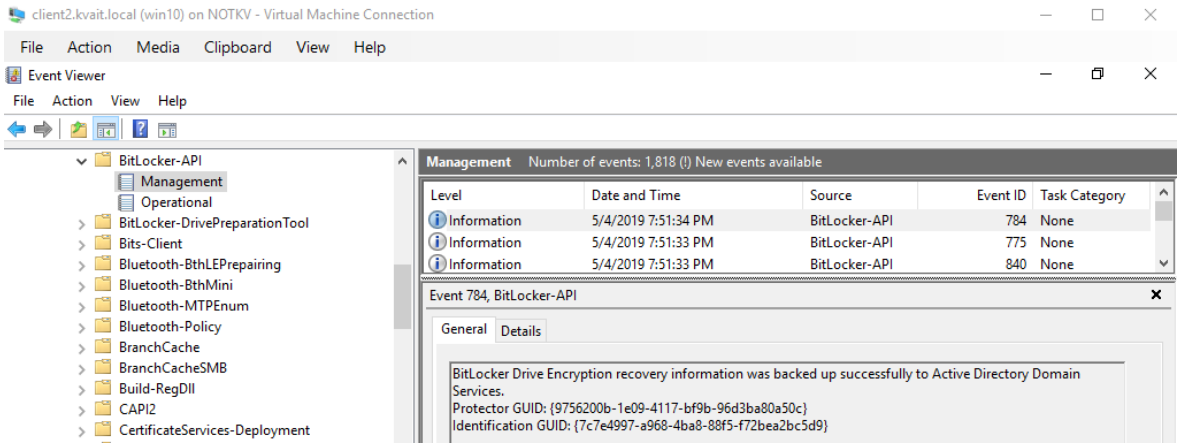
Obr. 46: Scenár č.2 – WDS, odpoveď na požiadavku klienta, vlastný zdroj.

7.3 Scenár č. 3

Testovací počítač (Client2.kvait.local), je rovnako ako v predošlom scenári členom domény a má nainštalovaného MBAM klienta. Rozdielna je však doménová skupinová politika, ktorá je na klientský počítač aplikovaná. Namiesto použitia dodatočnej formy autentifikácie (TPM + PIN), sa využíva iba samotný TPM modul.

Pri tomto scenári nie je nutná žiadna ďalšia manuálna konfigurácia na klientskej stanici. Šifrovanie vybraných diskových oddielov sa spustí automaticky po tom, ako sa na počítač úspešne aplikuje daná Bitlocker doménová skupinová politika a prebehne prihlásenie užívateľa. Užívateľ je na prebiehajúci proces šifrovania upozornený prostredníctvom informačnej „bubliny“ na systémovej lište. Zároveň bežný používateľ (bez administrátorských oprávnení), nemá možnosť zrušiť bežiaci proces šifrovania. Počas šifrovania sa na počítači dá naďalej bez problémov pracovať.

Samotný proces šifrovania sa považuje za úspešne ukončený až vtedy, keď je disk, zvolený diskový oddiel, alebo obsadený priestor na disku kompletne zašifrovaný. V tejto chvíli sa na základe nastavení v aplikovanej doménovej politike, automaticky uloží kľúč na obnovu do zvoleného úložiska.



Obr. 47: Scenár č.3 – Uloženie kľúča na obnovu, vlastný zdroj.

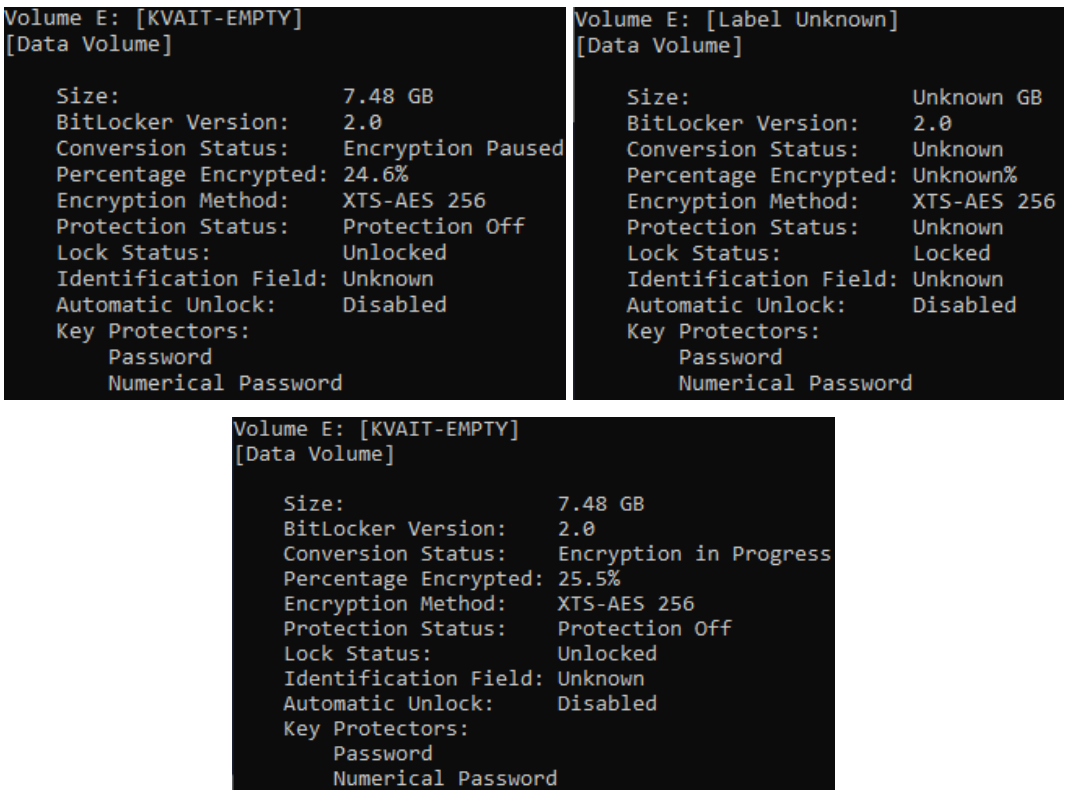
Výsledkom šifrovacieho procesu je disk zašifrovaný podľa parametrov definovaných systémovým administrátorom v doménovej skupinovej politike.

7.4 Scenár č. 4

Parametre Bitlocker To Go je možné rovnako ako parametre samotného Bitlocker nástroja konfigurovať prostredníctvom skupinových politík. V tomto prípade správca systému v skupinových politikách vynucuje jediné nastavenie - XTS–AES 256 bit. Bežný užívateľ, ktorý nie je správcom daného systému, nemá možnosť toto nastavenie modifikovať.

Po pripojení nezašifrovaného USB kľúča, bol cez ovládacie panely zapnutý Bitlocker To Go. Sprievodca nastaveniami, tak ako v scenároch uvedených vyššie, najprv požaduje, aby bola zvolená metóda, ako sa bude šifrovaný disk po pripojení do systému odomykať. Štandardne je v ponuke odomknutie pomocou hesla, alebo s použitím Smart karty. V ďalšom kroku je potom nutné uložiť kľúč na obnovu. Kľúč môže byť uložený do Microsoft konta, do súboru, alebo vytlačený. Posledný krok je voľba typu šifrovania (šifrovať iba obsadené miesto, alebo celý diskový oddiel).

Priebeh šifrovania je zobrazovaný rovnako ako v predošlých scenároch. Ak počas šifrovania užívateľ šifrovací proces pozastaví a kľúč zo systému odpojí, po následnom pripojení je požadované definované heslo. Po tom, ako užívateľ zadá platné heslo, šifrovanie pokračuje tam, kde naposledy skončilo.



Obr. 48: Scenár č.4 – Pozastavenie a pokračovanie šifrovania, vlastný zdroj.

7.5 Vyhodnotenie vhodnosti jednotlivých scenárov

Scenár č. 1, rieši správanie Bitlocker nástroja v základnej konfigurácii. Nie sú použité žiadne centrálne spravované politiky, a správca systému pri konfigurácii s použitím vstavaného sprievodcu vie využiť iba základnú funkcionalitu produktu. Riešenie je preto vhodné najmä pre zariadenia, ktoré nie sú členmi domény a neskúsenejších správcov.

Za **výhodu** môžeme považovať nenáročnú implementáciu. Na zašifrovanie disku nie je potrebné urobiť nič viac, iba krok za krokom prejsť jednotlivé nastavenia, ktoré ponúka vstavaný sprievodca

Naopak za **nevýhodu** tohto riešenia môžeme považovať problém s uchovaním kľúča na obnovu. Administrátor musí v tomto prípade nájsť bezpečný spôsob, ako kľúč uschovať a zabezpečiť. Ďalšou nevýhodou by mohla byť „sila“ použitého šifrovacieho algoritmu, ktorá je štandardne 128 bit. Toto nastavenie sa dá jednoducho zmeniť v registry databáze daného systému, ale to si už vyžaduje isté znalosti na strane administrátora daného systému.

Scenár č. 2, popisuje riešenie vhodné pre prostredia, kde je požadovaná zvýšená ochrana. Scenár kombinuje TPM s dodatočnou autentifikáciou s použitím PIN kódu (TPM + PIN) s funkcionalitou Network Unlock, ktorej cieľom je zabezpečiť zvýšený komfort koncového užívateľa systému.

Ako **výhody** v tomto prípade môžeme spomenúť napr.: bezpečné uchovanie kľúčov na obnovu, využitie PIN kódu, ako dodatočnej ochrany systému, možnosť centralizovanej správy a reportov, atď...

Asi najväčšou **nevýhodou** bude komplexnosť riešenia. Pri tomto scenári už nestačí iba nakonfigurovať koncovú stanicu, ale vyžaduje si rovnako konfiguračne a implementačné zmeny z pohľadu serverovej infraštruktúry.

Scenár č. 3, je v podstate akýmsi kompromisom medzi dvomi scenármi popísanými vyššie. Na jednej strane je tu isté zníženie nárokov a požiadaviek na samotnú implementáciu. Netreba napríklad riešiť certifikačnú autoritu v infraštruktúre spoločnosti a rovnako sa netreba zaoberať požiadavkami, ktoré sú nevyhnutné pre nasadenie Network Unlock funkcionality. Na druhej strane však spoločnosť príde o dodatočnú autentifikáciu vo forme PIN kódu. Tak ako pri predošlom scenári aj tu platí, že koncové počítače musia byť zaradené

v doméne a správca systému musí mať isté skúsenosti, aby bol schopný dané riešenie nasadiť.

Výhodami, ako už bolo spomenuté sú znížené požiadavky na implementáciu a celkovo serverovú infraštruktúru oproti scenáru č. 2. Zároveň ostávajú zachované základné atribúty požadované pre nasadenie vo firemnom prostredí, ako sú možnosti centrálnej správy, či reportovania. Ďalšou nespornou výhodou je, že disk na koncovej stanici (po splnení všetkých definovaných podmienok) sa zašifruje automaticky bez zásahu administrátora. Toto má za následok aj ďalšiu, zaujímavú vlastnosť – ak z nejakého dôvodu dôjde k vypnutiu šifrovania na koncovej stanici, po opätovnom načítaní doménových politík sa dešifrovaný disk začne opäť automaticky šifrovať.

Nevýhodou stále ostáva vyššia komplexnosť aj požiadavky na infraštruktúru, ako má scenár č. 1.

Scenár č. 4 je demonštráciou toho, ako je možné využiť Bitlocker nástroj v súvislosti s prenosnými pamäťovými médiami, ako sú napr. USB disky, či kľúče. Spoločnou črtou s predošlými dvomi scenármi je možnosť prispôsobenia Bitlocker nastavení firemným štandardom pomocou doménových politík. Zároveň je však rovnako dobre využiteľný v ne-doménovom prostredí, kde si užívateľ môže zašifrovať svoje prenosné disky aj sám bez pomoci systémového administrátora.

8 SPRÁVA SYSTÉMOV A ZÍSKANIE KĽÚČA NA OBNOVU

Pod bežnou správou v tomto prípade rozumieme dennú agendu správcov systémov vo firemnej sieti. V tejto kapitole sú zhrnuté kľúčové body a činnosti so zameraním na šifrovací nástroj Bitlocker.

V prípade nasadenia Bitlocker šifrovania je nevyhnutné, byť si vedomý možných udalostí, ktoré môžu spôsobiť, že šifrovaný disk sa stane neprístupným. Systémový správca musí mať preto v prípade potreby možnosť získať kľuč na obnovu. Rovnako je dôležité poznať úložisko týchto kľúčov a poznať spôsob, ako ho rozumne zabezpečiť pred nepovolanými osobami.

8.1 Režim obnovy

Zoznam najčastejších príčin, kedy je užívateľ vyzvaný na zadanie obnovovacieho kľúča:

- *„Presun Bitlockerom šifrovaného disku z jedného počítača do iného.*
- *Inštalácia novej základnej dosky, s novým TPM čipom.*
- *Vypnutie, zakázanie, alebo vymazanie TPM.*
- *Update BIOS/UEFI rozhraní, príp. zmeny v ich nastaveniach.*
- *Update ROM.*
- *Zabudnutie PIN (ak bola povolená dodatočná autentifikácia PIN kódom).*
- *Strata USB kľúča, ktorý obsahoval štartovací kľúč, ak bol povolený tento spôsob autentifikácie"[44].*

Je samozrejme odporúčané, aby BIOS, príp. UEFI rozhranie každého systému bolo chránené heslom, ktoré bežný užívateľ nepozná. Týmto opatrením sa dá predísť väčšine z vyššie uvádzaných problémov.

V prípade, že je potrebné na systéme vykonať zmeny, ktoré by mohli spôsobiť uzamknutie šifrovaného disku, je odporúčané šifrovanie na nevyhnutný čas pozastaviť[6]. Po skončení týchto aktivít správca šifrovanie opäť manuálne povolí a systém je znovu plne chránený.

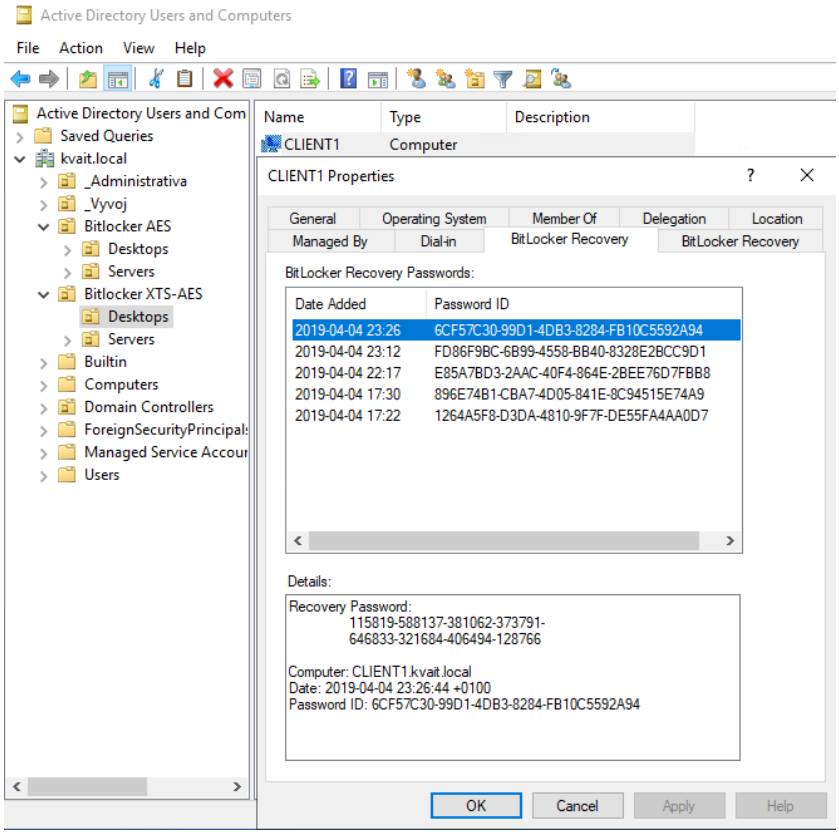
[6]témou pozastavenia Bitlocker šifrovania na zašifrovanom disku sa podrobnejšie zaoberá kapitola 8.4.

8.2 Vygenerovanie kľúča na obnovu

Tak, ako už bolo uvedené, po úspešnom zašifrovaní diskov, sú kľúče potrebné na obnovu automaticky uložene podľa zvolenej konfigurácie v doménových skupinových politikách. Úložiskom pritom môžu byť Adresárová Služba, alebo SQL Databáza.

8.2.1 Úložisko - Adresárová služba

Kľúč na obnovenie pre konkrétne zariadenie sa dá najjednoduchšie získať cez nadstavbu „Active Directory Users and Computers[7]“ konzoly. Systémový správca s dostatočnými oprávneniami si cez spomínanú konzolu vyhľadá konkrétny počítačový objekt a v jeho vlastnostiach na záložke „Bitlocker Recovery“ nájde požadovaný kľúč.



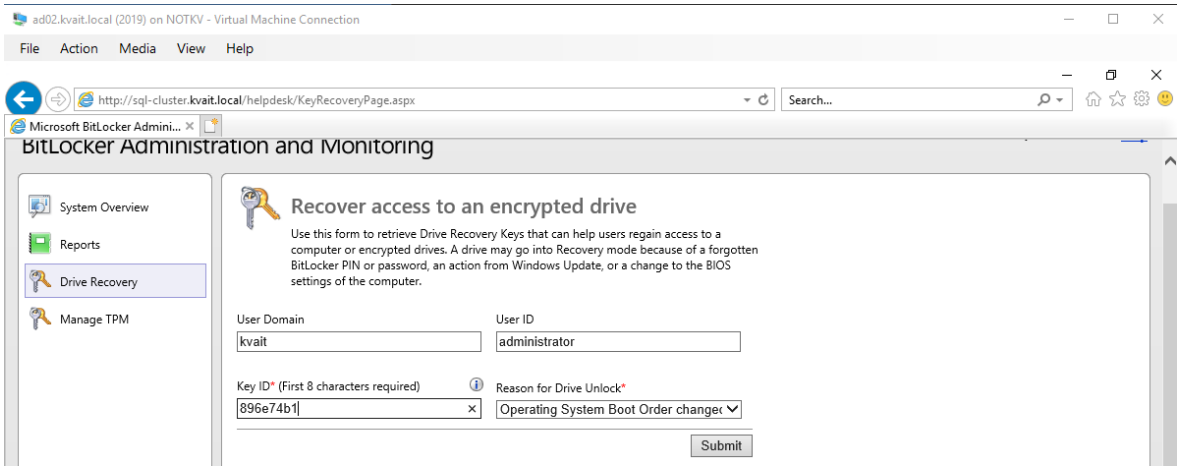
Obr. 49: Úložisko kľúča na obnovu – Adresárová služba, vlastný zdroj.

[7]Active Directory Users and Computers – je jedným z modulov Microsoft manažment konzoly pre správu Adresárových služieb (užívateľské a počítačové účty, organizačné jednotky, atď...).

8.2.2 Úložisko - SQL databáza

Z SQL databázy sa požadované kľúče dajú získať rôznymi spôsobmi. Jedným z najjednoduchších je využitie SQL dopytu priamo z „Microsoft SQL Server Management Studio[8]“ konzoly. Druhou, transparentnejšou možnosťou je využiť sprostredkované pripojenie pomocou Web servera. IIS služba na tomto serveri sa pripája do MBAM databázy a odtiaľto získava pre prihláseného správcu požadované informácie. V prípade tejto práce je „HelpDesk“ portál dostupný na adrese: **https://sql-cluster.kvait.local/helpdesk.**

V časti „Drive Recovery“ po vyplnení povinných informácií je systémovému administrátorovi zobrazený požadovaný obnovovací kľúč.



Obr. 50: Úložisko kľúča naobnovu – SQL Databáza, vlastný zdroj.

8.2.3 Ochrana úložísk

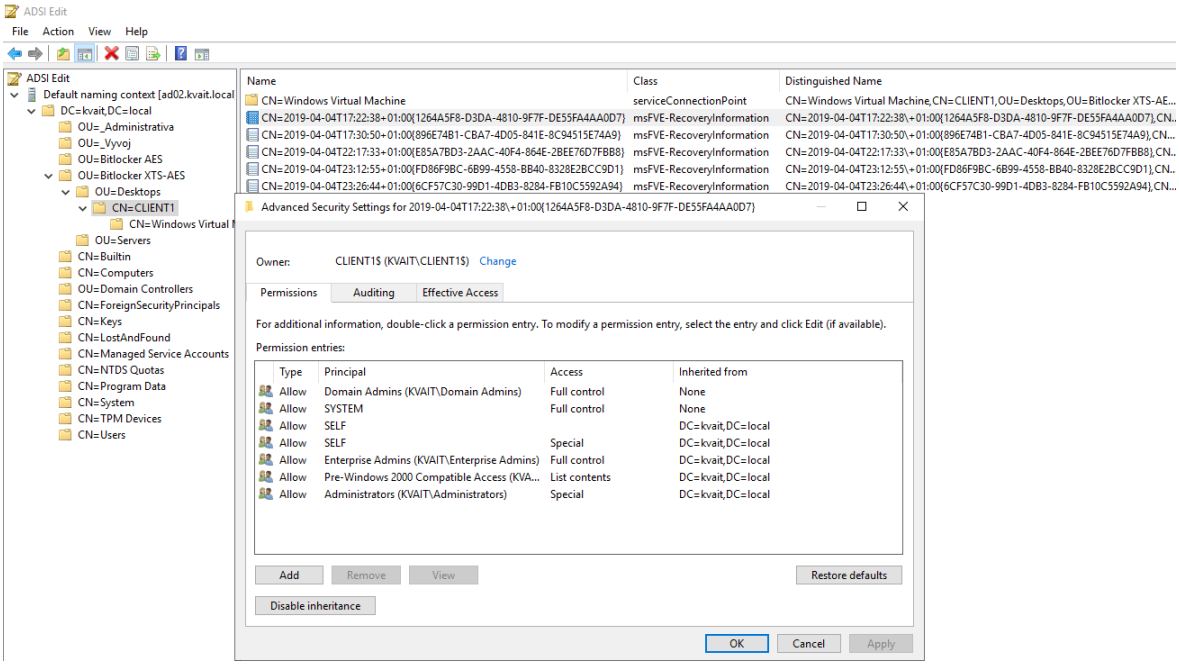
Jedným z najdôležitejších predpokladov pre plne funkčného a naozaj bezpečného nasadenia Bitlocker nástroja, je zabezpečiť aby nedošlo k diskreditácii úložiska kľúčov na obnovu. Ak útočník získa prístup k tomuto úložisku, celé šifrovanie stráca svoj význam. Jediným možným spôsobom, ako toto úložisko spoľahlivo zabezpečiť je skĺbenie bezpečnostných prvkoch na hardvérovej (fyzickej) aj softvérovej úrovne. Náplňou tejto práce však nie je posudzovať fyzickú bezpečnosť systémov, preto budú v tejto kapitole spomenuté iba bezpečnostné prvky na softvérovej úrovni.

[8]Microsoft SQL Server Management Studio – *„je integrované prostredie pre správu SQL infraštruktúry, ktoré poskytuje nástroje na konfiguráciu, monitorovanie a správu SQL inštancií na databázovom serveri“ [45].*

V rámci **Adresárových služieb** je z pohľadu Bitlocker nástroja zaujímavá Class (trieda atribútov) z názvom: **ms-FVE-RecoveryInformation.**

Na tomto mieste sa dajú nájsť informácie ohľadom Bitlocker kľúča na obnovenie pre konkrétne zariadenie. Zároveň a čo je velmi dôležite, je možné pre túto Class delegovať oprávnenia. Delegáciou oprávnení iba pre konkrétných administrátorov je správca schopný zamedziť voľnému prístupu k týmto citlivým informáciám.

Ďaľšou dôležitou vlastnosťou je možnosť auditingu. Ak to organizácia s nasadením Bitlocker šifrovania myslí vážne, je nevyhnutné, aby auditovala a archivovala prístup ku obnovovacím kľúčom.



Obr. 51: Adsi edit[9] – Bitlocker kľúč na obnovu, vlastný zdroj.

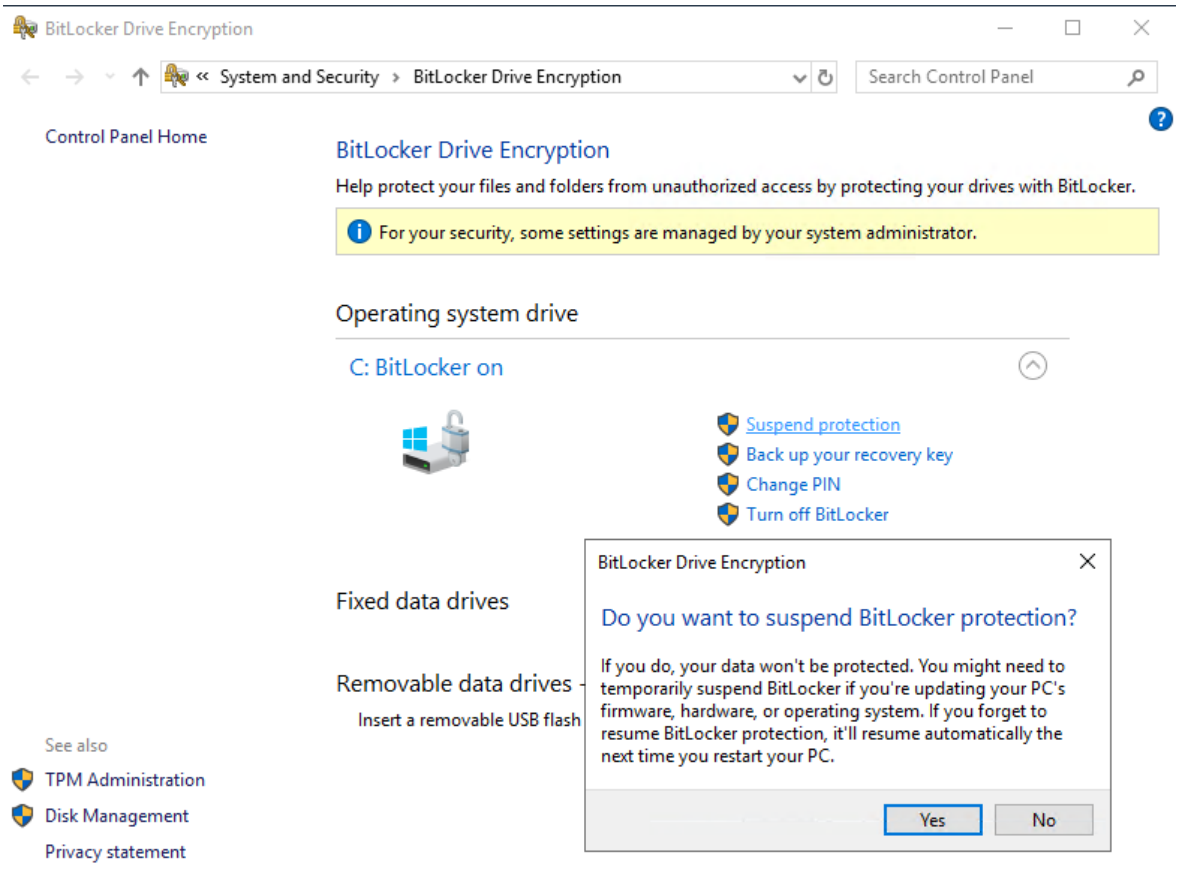
Údaje uložené v **Microsoft SQL** databázach je možné zabezpečiť pomocou prístupových oprávnení. V tejto práci boli pre tento účel vytvorené tri rôzne doménové skupiny (viď kap. 6.1.1.1). Pre každú jednu databázu, je možné definovať rôzne úrovne prístupu a tým zabezpečiť, aby neboli údaje voľne dostupné pre každého, komu sa podarí k danej databáze pripojiť.

[9]Adsi edit – je Microsoft manažment konzola určená na nízko-úrovňové spravovanie Adresárových služieb.

8.3 Pozastavenie a vypnutie ochrany

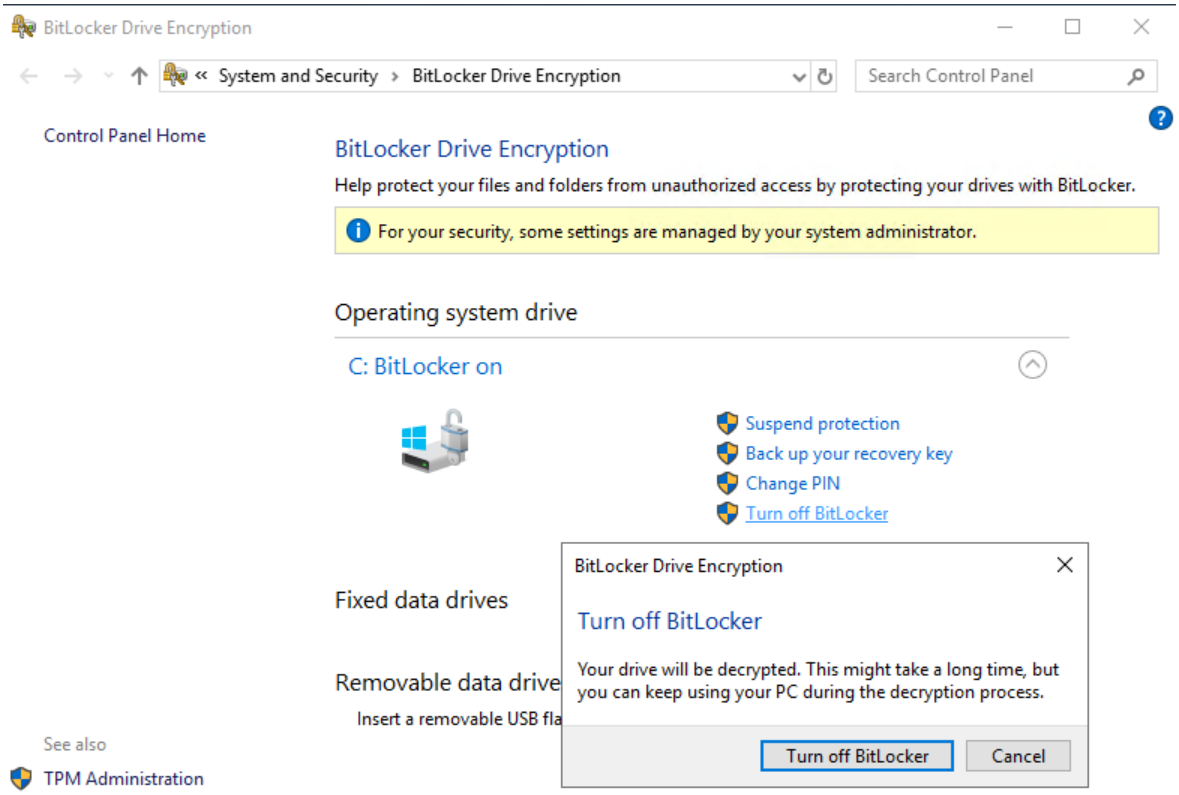
Na úvod je dôležité ozrejmiť, aký je vlastne rozdiel medzi pozastavením Bitlocker ochrany a jej vypnutím.

Pozastavením rozumieme proces, kedy sa z nejakého dôvodu predpokladá narušenie integrity jedného s komponentov, ktoré by malo za následok nedostupnosť šifrovaných dát a následne žiadosť o zadanie kľúča na obnovu. V praxi sa táto situácia najčastejšie vyskytuje pri aplikácii rôznych aktualizácií, záplat, či firmvérov. Pri pozastavení ochrany na rozdiel od jej vypnutia, nedochádza k dešifrovaniu šifrovaného disku, alebo jeho časti. Šifrovacie kľúče sú v tomto prípade jednoduchšie prístupné a preto je nevyhnutné, aby správca systému mal celý čas takýto systém pod kontrolou. Kľúčovou je v tejto situácii istá „disciplína“, aby sa predišlo zbytočnému narušeniu bezpečnosti a šifrovanie by malo byť opätovne povolené hneď, ako je to možné.



Obr. 52: Pozastavenie Bitlocker ochrany, vlastný zdroj.

Vypnutie Bitlocker šifrovania spôsobí spustenie dešifrovacieho procesu. Po tom, čo je proces úspešne ukončený[10], je Bitlocker nástroj vypnutý a disk v nešifrovanej forme. Jedným z mála objektívnych dôvodov, kedy je vhodné vypnúť ochranu, je scenár, kedy bol na danom systéme v minulosti použitý slabší šifrovací algoritmus a po dešifrovaní celého disku, ho následne správca zašifruje použitím nového, silnejšieho algoritmu.



Obr. 53: Vypnutie Bitlocker ochrany, vlastný zdroj.

Z textu vyššie vyplýva, že v organizácii, kde bolo Bitlocker šifrovanie nasadené za istým účelom, je cieľom používať pozastavenie ochrany iba v nevyhnutných prípadoch a jednoznačne zabrániť bezdôvodnému vypínaniu Bitlocker nástroja. Preto je obzvlášť dôležité, aby administrátorské oprávnenia na jednotlivých systémoch boli pridelené iba osobám, ktoré ich reálne potrebujú a nie bežným užívateľom. Pretože bežný užívateľ systému nemá štandardne právo ochranu ani pozastaviť ani vypnúť, rapídne tým v tomto smere znížime možnosti narušenia bezpečnosti.

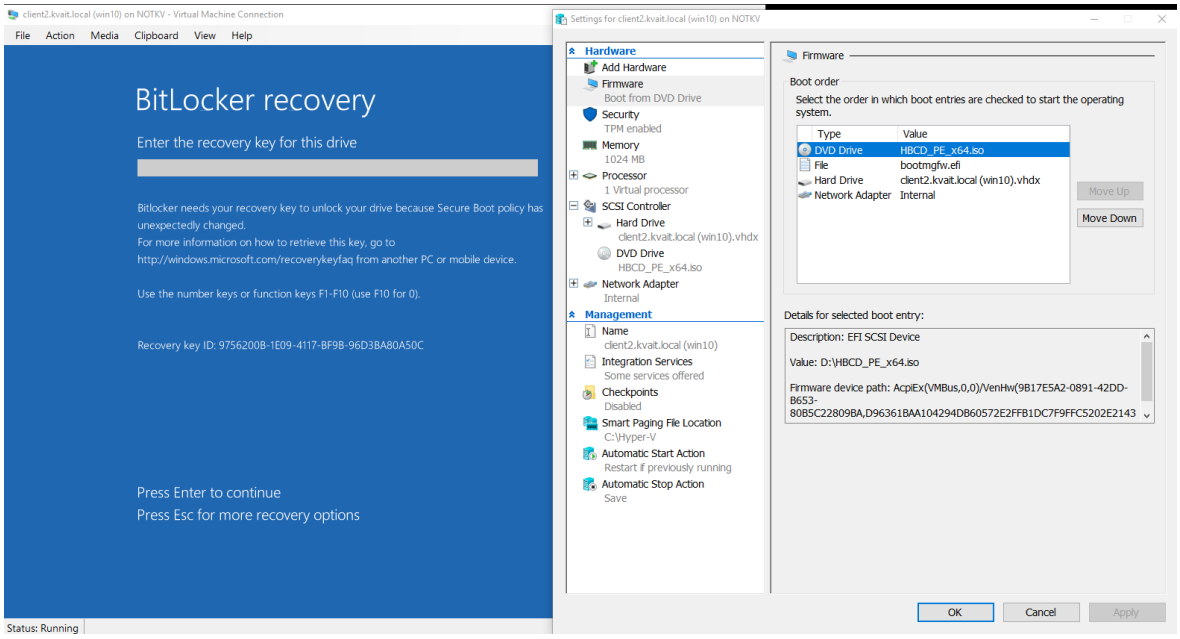
[10]dĺžka trvania dešifrovacieho procesu závisí hlavne od veľkosti disku, množstva šifrovaných dát a hardvéru daného zariadenia.

9 SPRÁVANIE SA SYSTÉMU V BEŽNEJ PREVÁDZKE

Cieľom tejto kapitoly je na niekoľkých vzorových príkladoch ukázať, ako sa bude správať disk šifrovaný nástrojom Bitlocker v rôznych situáciách, ku ktorým môže dôjsť počas bežnej prevádzky. Prvá kapitola hovorí o tom, že v podstate jednoduchá zmena v nastavení UEFI rozhrania spôsobí, že od užívateľa je požadované zadanie kľúča na obnovu. Ďalšia kapitola demonštruje, ako sa správa šifrovaný disk, ak je presunutý z počítača obete do počítača útočníka. Cieľom poslednej kapitoly je opäť poukázať na to, aké dôležité je zabezpečiť, aby bežný užívateľ na svojom firemnom počítači nemal priradené práva lokálneho administrátora.

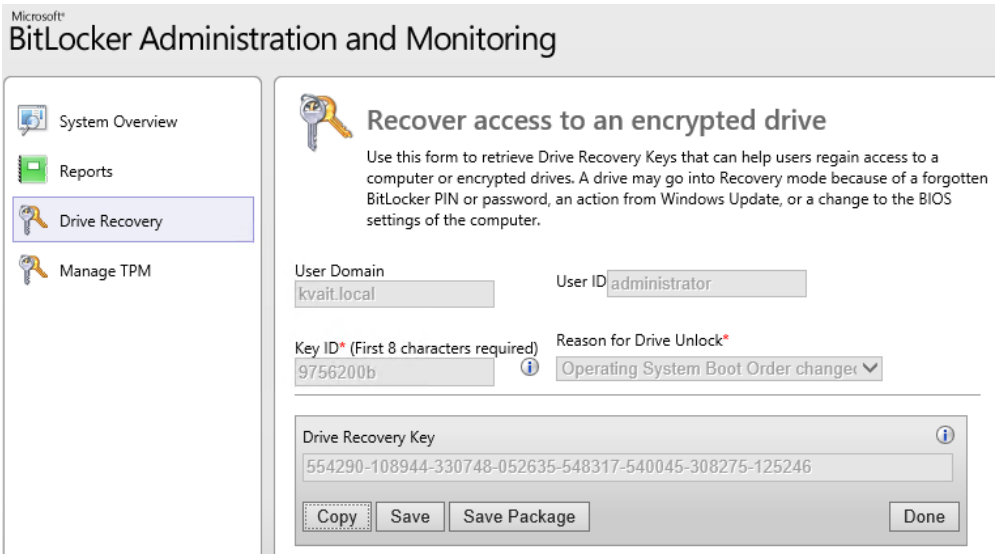
9.1 Zmena v nastavení UEFI rozhrania

Táto zmena je demonštrovaná na virtuálnom počítači, kde bol do DVD mechaniky vložený ISO obraz inštalačného média a bolo zmenené poradie zariadení (BOOT order), z ktorých sa bude snažiť načítať operačný systém. Zmena v konfigurácii v tomto prípade spôsobí narušenie integrity procesu zavádzania a od užívateľa je požadované kľúč na obnovu.



Obr. 54: Zmena v nastavení UEFI rozhrania, vlastný zdroj.

Prvých 8 znakov z „Recovery Key ID“, ktoré sa zobrazí na obrazovke po zapnutí klientskej stanice, sa použije na MBAM web stránke na vygenerovanie kľúča na obnovu. Vygenerovaný kľúč na obnovu (Drive Recovery Key) sa následne zadá priamo na klientskom počítači a tým sa spustí samotné zavádzanie operačného systému.

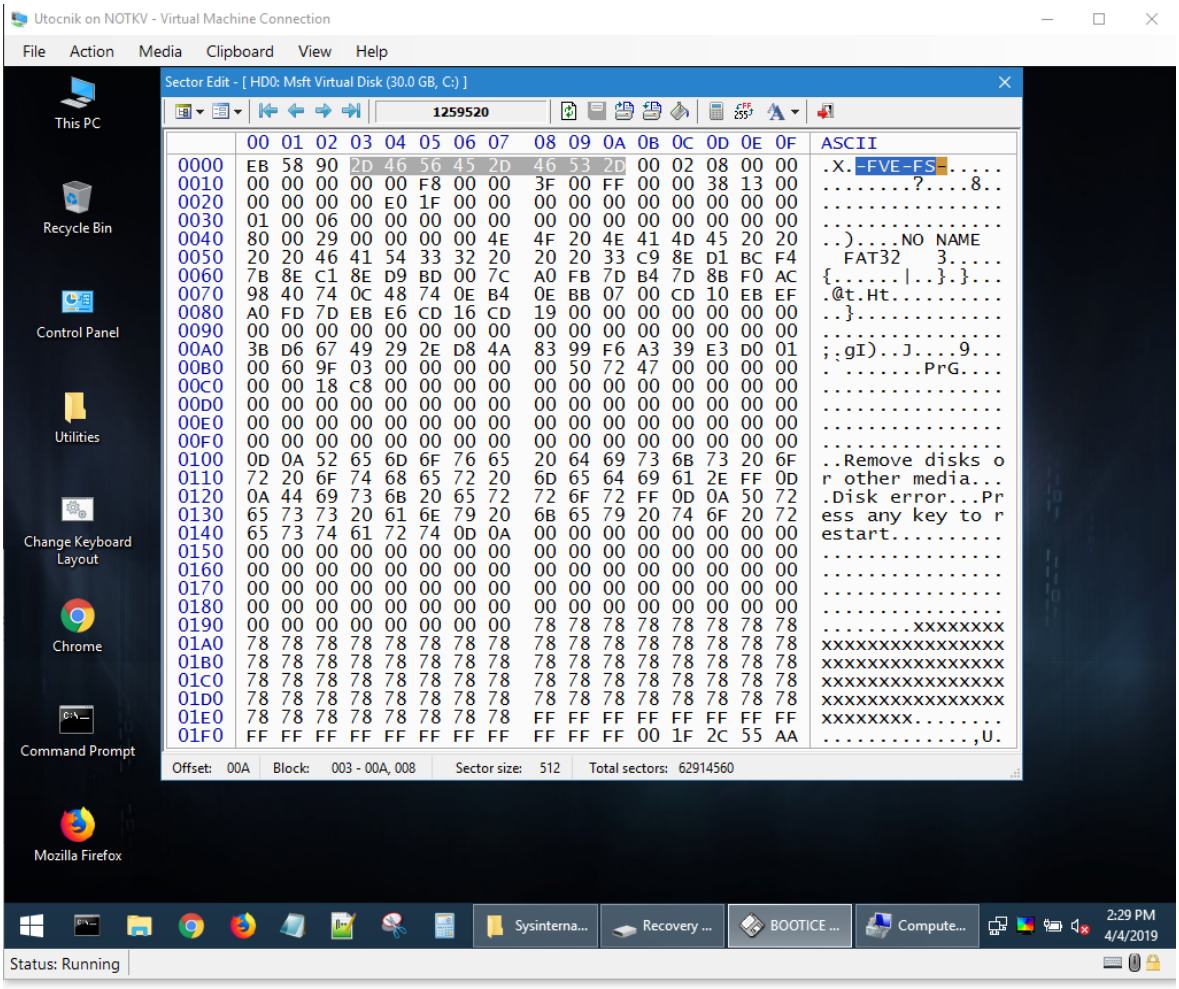


Obr. 55: MBAM web – vygenerovanie kľúča na obnovu, vlastný zdroj.

9.2 Presun disku do iného počítača

Šifrovaný disk z Client1 virtuálneho počítača bol priradený virtuálnemu počítaču – Utocnik. Systém bol naštartovaný pomocou „Hirens Boot CD“ média. Obsah šifrovaného disku bol nečitateľný. Pomocou nízko-úrovňového nástroja schopného priamo čítať obsah jednotlivých sektorov na danom disku je možné vidieť signatúru Bitlocker šifrovacieho nástroja na disku. Nič to ale nemení na fakte, že dáta sú aj na tejto úrovni neprístupné.

Situácia by bola samozrejme totožná aj v prípade, že by sa jednalo o presun šifrovaného disku z jedného fyzického počítača do iného.

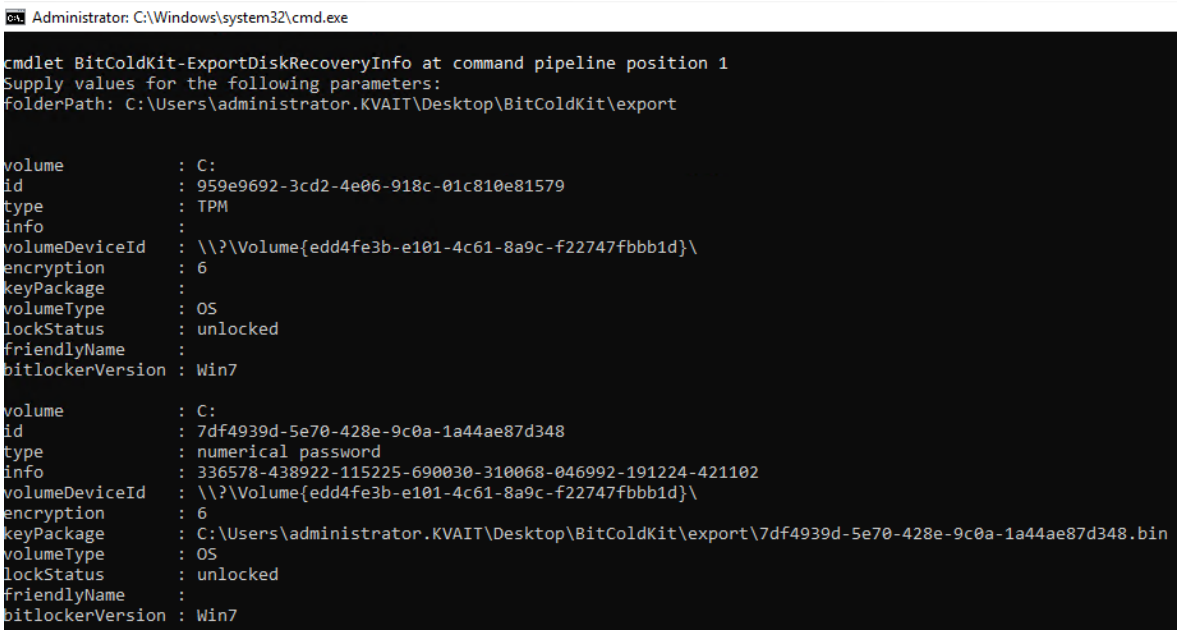


Obr. 56: Signatúra Bitlocker nástroja na šifrovanom disku, vlastný zdroj.

9.3 Extrakcia kľúča na obnovu z pamäte počítača

Je samozrejmé, že zásadnou podmienkou toho, aby sa s pevným diskom dalo normálne pracovať, musí byť v „odomknutom“ stave. Bitlocker šifrovaný disk je v tomto stave vždy, keď je počítač zapnutý a spustený operačný systém Microsoft Windows. Kľúč na obnovu je pritom uložený v operačnej pamäti počítača. V tejto chvíli prichádza na scénu toľko krát spomínaná situácia – na jednej strane oprávnenia bežného užívateľa a na strane druhej, oprávnenie správcu systému.

Existuje mnoho voľne dostupných nástrojov, ktoré sú schopné vyextrahovať citlivé údaje z operačnej pamäte zapnutého počítača. Všetky však pre svoju prácu potrebujú dostatočné oprávnenia na danom systéme. Ak osoba, ktorá na počítači bežne pracuje nemá administrátorské oprávnenia, je skoro nemožné takéto nástroje použiť.



Obr. 57: BitColdKit[11] – Extrakcia kľúča na obnovu z pamäte, vlastný zdroj.

[11]BitColdKit – voľne dostupný nástroj schopný z operačnej pamäte počítača získať citlivé údaje ohľadom Bitlocker šifrovaného disku [46].

9.4 Vyhodnotenie kapitoly

Ak sa počas bežnej prevádzky dodržiavajú odporúčania, ktoré so sebou prináša implementácia Bitlocker šifrovania a hlavne má organizácia nasadený a funkčný model užívateľských oprávnení, potom sa pre koncového užívateľa v zásade nič nemení. Za istých okolností si ani nemusí všimnúť, že je nejaké šifrovanie vôbec nasadené. Problém nastáva vo chvíli, keď je niektorý z vyššie uvedených faktorov nefunkčný. Problémy ako každodenné žiadosti o generovanie obnovovacích kľúčov, alebo sťažnosti pracovníkov na nefunkčnosť systému potom môžu ľahko viesť k situáciám, kedy sú neúmyselne prehliadané dôležité bezpečnostné incidenty a eskalácie oprávnení.

Čo sa týka zmien v nastavení UEFI rozhrania, pri určitých činnostiach sa týmto zmenám zabrániť samozrejme nedá. V tej chvíli ale systémový správca má stále možnosť na nevyhnutne potrebný čas šifrovanie disku pozastaviť.

Scenár, kedy je šifrovaný disk v inom počítači nečitateľný je požadovaný stav a presne to, čo sa od Bitlocker nástroja očakáva.

Extrakcia citlivých údajov z operačnej pamäte v globále (nielen Bitlocker kľúčov), je nežiadúci stav, ktorému by sa mala každá organizácia snažiť v čo možno najväčšej miere predísť.

Okrem už spomínaných nástrojov a techník je dôležité do pravidelných činností správcov jednotlivých systémov zaradiť aj kontrolu výstupov z monitorovacích nástrojov (ak sú v organizácii nasadene), kontrolu denníkov udalostí minimálne tých najdôležitejších systémov a samozrejme reportov samotného Bitlocker nástroja.

ZÁVER

Jedným zo základných predpokladov na to, aby bol daný produkt, systém či samotné riešenie akceptované užívateľmi, je, aby bolo pre nich pokiaľ možno „neviditeľné“. Iné požiadavky samozrejme vyžaduje vedenie spoločnosti, iné budú mať osoby zodpovedné za bezpečnosť a iné správcovia daných systémov, ktorí sú zodpovední za každodennú správu. Tieto riadky sa v globále dajú použiť pre každé jedno riešenie. V svojej práci som sa snažil práve tieto požiadavky preniesť do praxe v súvislosti s nasadením nástroja na šifrovanie diskov. Zvolil som také konfigurácie a scenáre nasadenia, ktoré sú reálne použiteľné v praxi. Cieľom bolo popísať princípy, jednotlivé možnosti ich výhody, ale zároveň upozorniť aj na možné nevýhody.

Praktická časť sa začína popisom už existujúceho virtuálneho prostredia, vytvoreného tak, aby bolo čo možno najbližšie reálnym podmienkam. Posledné roky v IT segmente potvrdzujú masívny vzostup virtualizačnej platformy a spoločnosti čím ďalej tým viac prechádzajú na virtualizované systémy. Preto je zvolené riešenie s malými obmenami možné kedykoľvek využiť v reálnom živote.

V kapitole 7, sú popísané štyri vybrané scenáre nasadenia. Prvý až tretí hovoria o využití Bitlocker nástroja na šifrovanie pevného disku klientského počítača. Popísané sú podrobné postupy zašifrovania disku s použitím vstavaného sprievodcu a možnosti prispôsobenia šifrovania požiadavkám správcu systému. Scenár č. 4, demonštruje využitie nástroja Bitlocker To Go. Kapitolu uzatvára vyhodnotenie vhodnosti a parametrov jednotlivých scenárov.

Po nasadení každého riešenia prichádza na rad každodenná, alebo inak povedané bežná správa. Systémový správca musí vedieť, kedy sa systém so zašifrovaným diskom môže dostať do tzv. Režimu obnovy, keď je od užívateľa požadovaný kľúč na obnovu. Dôležité je takisto vedieť, kde sú tieto kľúče uložené a aká je ochrana týchto úložísk. Súčasťou práce administrátora je rovnako inštalácia rôznych aplikácií, aplikovanie pravidelných aktualizácií, či záplat. Je preto nevyhnutné aby sa dala ochrana pozastaviť.

Posledná časť práce rozoberá prípady, ako sa systém zachová, keď sa zmenia nastavenia UEFI rozhrania, alebo keď sa presunie pevný disk z jedného virtuálneho počítača (počítač obete) do iného počítača (počítač útočníka). Kapitola demonštruje, že dáta naozaj nie sú útočníkovi prístupné a to ani v prípade prístupu pomocou nízko-úrovňových nástrojov. Časť ohľadom extrakcie Bitlocker kľúčov z pamäte bežiaceho systému pripomína

toľko zdôrazňované pravidlo, ohľadom ochrany administrátorských oprávnení. Praktickú časť uzatvára krátke vyhodnotenie predošlých kapitol.

V kontexte tejto práce sa Bitlocker ukázal ako použiteľný a dostatočne konkurencieschopný nástroj na šifrovanie diskov a prenosných pamäťových médií. Najväčšie výhody vidím v integrácii tohto nástroja vo vybraných verziách Microsoft operačných systémoch a tým pádom aj dobrej podpore zo strany výrobcu. Sila šifrovacích algoritmov, ako aj úroveň a jednoduchosť ovládania sú taktiež na dobrej úrovni. S príchodom XTS-AES 256bit výrobca urobil veľký posun z hľadiska bezpečnosti. Možnosť skombinovať dodatočnú ochranu kľúča pomocou PIN kódu a funkcionalitou Network Unlock, je vo firemnom prostredí veľmi zaujímavou alternatívou. Nevýhodu vidím v tom, že Bitlocker je voľne dostupný iba pre užívateľov vybraných edícií klientských operačných systémov. Bežný domáci užívateľ preto štandardne tento nástroj nemôže využiť.

Ohľadom využitia centralizovanej správy, treba počítať s tým, že MBAM nie je voľne dostupný a je súčasťou konkrétnych licenčných programov spoločnosti Microsoft. Čo sa týka funkčnej stránky, v čase písanie nepodporuje všetky funkcie, ktoré poskytuje Bitlocker v nových verziách Windows operačných systémoch. Z tohto dôvodu je nevyhnutné požadované parametre nastavovať na viacerých miestach (rôzne vetvy doménových skupinových politík) a tým sa správa zbytočne komplikuje. Ďalší problém predstavujú reporty. V štandardnom nastavení tým, že MBAM nepodporuje najnovšie XTS-AES šifrovanie, je klient ktorý tieto algoritmy využíva zobrazený ako problémový. V tejto chvíli je rovnako otázna budúca podpora MBAM nástroja. Štandardná podpora oficiálne končí 9.7.2019. Či bude produkt zo strany výrobcu rozširovaný a aktualizovaný aj ďalej je preto otázne.

Využitie Bitlocker nástroja z pohľadu organizácie, kde je prevažná časť systémov na platforme Microsoft a spoločnosť má zaplatený potrebný licenčný program vnímam ako veľmi vhodný. Pri ostatných organizáciách je potrebné si pred samotnou implementáciou zvážiť všetky pozitívne a negatívne stránky produktu. Pre bežného domáceho užívateľa, kde produkt nie je súčasťou operačného systému bude výhodnejšie siahnuť po jednej z voľne dostupných alternatív.

ZOZNAM POUŽITEJ LITERATÚRY

[1] MULLEN Timothy. *Thor's Microsoft Security Bible: A Collection of Practical Security Techniques.* United States of America: Elsevier, 2011. ISBN 978-1-59749-572-1.

[2] YOSIFOVICH Pavel, Mark E. RUSSINOVICH, David A. SOLOMON, Alex IONESCU. *Windows Internals Part 1: System architecture, processes, threads, memory management, and more. Seventh edition.* Redmond: Microsoft, [2017). ISBN 978-0-73568-418-8. https://archive.org/details/windows-internals-part1-7th.

[3] RUSSINOVICH Mark, David A. SOLOMON a Alex IONESCU. *Windows Internals: Part 2. 6th Edition.* United States of America: Microsoft Press, 2012. ISBN 978-0-7356-6587-3.

[4] MINASI Mark, Kevin GREENE, Robert BUTLER, John MCCABE, Robert PANEK, Michael RICE, Stefan ROTH a Christian BOOTH. *Sybex: Mastering Windows Server 2012 R2.* Indianapolis, Indiana: John Wiley & Sons, 2014. ISBN 978-1-118-33172-9.

[5] WARNER Timothy a Craig ZACKER. *Securing Windows Server 2016: Exam Ref 70-744*. United States of America: Pearson Education, 2017. ISBN 978-1-5093-0426-4.

[6] *Microsoft. Windows IT Pro Center: Bitlocker. Bitlocker (Windows 10): Microsoft Docs* [online]. 2017. Dostupné z: https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview.

[7] MIŠÁNEK, Martin. *Analýza nástrojov na šifrovanie pevných diskov* [online]. Banská Bystrica, 2015 [cit. 2019-05-01]. Dostupné z: https://is.ambis.cz/th/oy9mv/BP_Misanek_v09.pdf. Bakalárska práca. Bankovní institut vysoká škola Praha, zahraničná vysoká škola Banská Bystrica. Vedoucí práce Ing. Radoslav Forgáč, PhD.

[8] Advanced Encryption Standard. In: *Wikipedia: the free encyclopedia*[online]. San Francisco (CA): Wikimedia Foundation, 2019 [cit. 2019-05-01]. Dostupné z: https://cs.wikipedia.org/wiki/Advanced_Encryption_Standard.

[9] *Šifrovanie pre bezpečnosť údajov - GDPR: Nové všeobecné nariadenie EÚ o ochrane údajov (GDPR)* [online]. [cit. 2019-05-01]. Dostupné z: https://encryption.eset.com/sk/sifrovanie-kluce-a-bezpecnost-udajov/.

[10] SOSNOWSKI, Rafal. *Microsoft Technet | Dubai Security Blog: Bitlocker: AES-XTS (new encryption type)* [online]. 2016 [cit. 2019-05-01]. Dostupné z: https://blogs.technet.microsoft.com/dubaisec/2016/03/04/bitlocker-aes-xts-new-encryption-type/.

[11] *DTCA: Princípy bezpečnej komunikácie* [online]. 2005 [cit. 2019-05-01]. Dostupné z: http://www.dtca.sk/support/principles.php.

[12] KMENT, Vojtěch. *Hašovací funkce: Jak se odolává hackerům* [online]. 2005 [cit. 2019-05-01]. Dostupné z: https://www.lupa.cz/clanky/hasovaci-funkce-jak-se-odolava-hackerum/.

[13] ŽÚBOR, Peter. *Informačné systémy pre riadenie identít a riadenie prístupu v organizácii* [online]. Banská Bystrica, 2014 [cit. 2019-05-01]. Dostupné z: https://is.ambis.cz/th/pklf4/Informacne_systemy_pre_riadenie_identit_a_riadenie_pristupu_v_organizacii.pdf. Bakalárska práca. Bankovní institut vysoká škola Praha, zahraničná vysoká škola Banská Bystrica. Vedoucí práce Ing. Miroslav Gecovič, CSc.

[14] KOPÁČ, Peter. *Jednotná autentifikácia používateľov webových aplikácií na UK* [online]. Bratislava, 2007 [cit. 2019-05-01]. Dostupné z: http://www.dcs.fmph.uniba.sk/diplomovky/obhajene/getfile.php/kopac_diplomovka_locked.pdf?id=147&fid=239&type=application%2Fpdf. Diplomová Práca. Univerzita Komenského, Bratislava. Vedoucí práce Mgr. Pavol Mederly.

[15] SMEJKAL, Miroslav. *Forenzní analýzy šifrovaných dat* [online]. Zlín, 2015 [cit. 2019-05-01]. Dostupné z: https://digilib.k.utb.cz/bitstream/handle/10563/31894/smejkal_2015_dp.pdf?sequence=1&isAllowed=y. Diplomová práce. Univerzita Tomáše Bati ve Zlíně. Vedoucí práce Ing. David Malaník, Ph.D.

[16] *Microsoft. Windows IT Pro Center: Overview of BitLocker Device Encryption in Windows 10: Microsoft Docs* [online]. 2019 [cit. 2019-05-01]. Dostupné z: https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-device-encryption-overview-windows-10.

[17] MEIJER, Carlo a Bernard VAN GASTEL. *Self-encrypting deception: weaknesses in the encryption of solid state drives (SSDs)* [online]. Radboud University, the Netherlands, 2018 [cit. 2019-05-01]. Dostupné z: https://www.ru.nl/publish/pages/909282/draft-paper.pdf.

[18] *Trusted Computing Group: Trusted Platform Module (TPM) Summary* [online]. United States of America, 2008 [cit. 2019-05-01]. Dostupné z: https://trustedcomputinggroup.org/resource/trusted-platform-module-tpm-summary/.

[19] *Microsoft. Windows IT Pro Center: TPM fundamentals: Microsoft Docs* [online]. 2017 [cit. 2019-05-01]. Dostupné z: https://docs.microsoft.com/en-us/windows/security/information-protection/tpm/tpm-fundamentals.

[20] FUTRAL William a James GREENE. *SpringerLink: Fundamental Principles of Intel® TXT* [online]. Apress, Berkeley, CA, 2013 [cit. 2019-05-01]. Dostupné z: https://link.springer.com/chapter/10.1007/978-1-4302-6149-0_2.

[21] *Microsoft. Windows IT Pro Center: Understanding PCR banks on TPM 2.0 devices: Microsoft Docs* [online]. 2017 [cit. 2019-05-01]. Dostupné z: https://docs.microsoft.com/en-us/windows/security/information-protection/tpm/switch-pcr-banks-on-tpm-2-0-devices.

[22] *Microsoft. Windows IT Pro Center: Bitlocker: Microsoft Docs* [online]. 2014 [cit. 2019-05-01]. Dostupné z: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-8.1-and-8/dn641993(v%3dws.11).

[23] *Microsoft. Windows IT Pro Center: What's new in Windows 10, versions 1507 and 1511: Microsoft Docs* [online]. 2017 [cit. 2019-05-01]. Dostupné z: https://docs.microsoft.com/en-us/windows/whats-new/whats-new-windows-10-version-1507-and-1511#bitlocker.

[24] *Identita a prístup. Windows Server 2008 R2* [online]. Microsoft [cit. 2019-05-01]. Dostupné z: https://www.microsoft.com/slovakia/windowsserver2008/identity-access.aspx.

[25] BitLocker. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2019 [cit. 2019-05-01]. Dostupné z: https://en.wikipedia.org/wiki/BitLocker.

[26] *Microsoft Premier WorkshopPLUS Materials. Deploying and Managing BitLocker in the Enterprise: BitLocker Fundamentals*. Microsoft, 2014 [cit. 2019-05-01].

[27] ULÍK, Boris. *Windows User Group, Slovak Republic: Bitlocker* [online]. 2011 [cit. 2019-05-01]. Dostupné z: https://www.wug.sk/?name=blog&id=166_BitLocker.

[28] *Microsoft Premier WorkshopPLUS Materials. Windows 7 Essentials: Security.* Microsoft, 2009 [cit. 2019-05-01].

[29] *Microsoft. Windows IT Pro Center: Secure the Windows 10 boot process: Microsoft Docs* [online]. 2018 [cit. 2019-05-01]. Dostupné z: https://docs.microsoft.com/en-us/windows/security/information-protection/secure-the-windows-10-boot-process.

[30] Rootkit. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001-, 2018 [cit. 2019-05-01]. Dostupné z: https://cs.wikipedia.org/wiki/Rootkit.

[31] VAN BEERS, Twan. *NeroBlanco End-to-End IT Migration: Bitlocker Boot Process* [online]. England, Wales, 2016 [cit. 2019-05-01]. Dostupné z: https://www.neroblanco.co.uk/2016/12/advanced-windows-security-week-3/bitlocker-boot-process/.

[32] *Microsoft. Windows IT Pro Center: About MBAM 2.5: Microsoft Docs* [online]. 2016 [cit. 2019-05-01]. Dostupné z: https://docs.microsoft.com/en-us/microsoft-desktop-optimization-pack/mbam-v25/about-mbam-25.

[33] *Microsoft. Windows IT Pro Center: MBAM 2.5 Server Prerequisites for Stand-alone and Configuration Manager Integration Topologies: Microsoft Docs* [online]. 2016 [cit. 2019-05-01]. Dostupné z: https://docs.microsoft.com/en-us/microsoft-desktop-optimization-pack/mbam-v25/mbam-25-server-prerequisites-for-stand-alone-and-configuration-manager-integration-topologies.

[34] *Microsoft. Windows IT Pro Center: Prerequisites for MBAM 2.5 Clients: Microsoft Docs* [online]. 2016 [cit. 2019-05-01]. Dostupné z: https://docs.microsoft.com/en-us/microsoft-desktop-optimization-pack/mbam-v25/prerequisites-for-mbam-25-clients.

[35] *Microsoft. Windows IT Pro Center: High-Level Architecture of MBAM 2.5 with Stand-alone Topology: Microsoft Docs* [online]. 2016 [cit. 2019-05-01]. Dostupné z: https://docs.microsoft.com/en-us/microsoft-desktop-optimization-pack/mbam-v25/high-level-architecture-of-mbam-25-with-stand-alone-topology.

[36] VAIT Karol. *Zabezpečení v prostředí Microsoft Active Directory* [online]. Zlín, 2017 [cit. 2019-05-01]. Dostupné z: https://digilib.k.utb.cz/bitstream/handle/10563/40833/vait_2017_dp.pdf?sequence=1&isAllowed=y. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně. Vedoucí práce Doc. Ing. Martin Sysel, Ph.D.

[37] SOSNOWSKI Rafal. *Microsoft Technet | Dubai Security Blog: Bitlocker: Network Unlock* [online]. 2016 [cit. 2019-05-01]. Dostupné z: https://blogs.technet.microsoft.com/dubaisec/2016/04/14/bitlocker-network-unlock/.

[38] *Microsoft. Windows IT Pro Center: BitLocker To Go FAQ: Microsoft Docs* [online]. 2018 [cit. 2019-05-01]. Dostupné z: https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-to-go-faq.

[39] *ForensicsWiki: BitLocker Disk Encryption* [online]. 2016 [cit. 2019-05-01]. Dostupné z: https://www.forensicswiki.org/wiki/BitLocker_Disk_Encryption.

[40] *VeraCrypt* [online]. [cit. 2019-05-01]. Dostupné z: https://www.veracrypt.fr/en/Home.html.

[41] *Symantec Encryption Desktop for Windows: Quick Start Guide* [online]. Verzia 10.3, 2013 [cit. 2019-05-01]. Dostupné z: https://origin-symwisedownload.symantec.com/resources/sites/SYMWISE/content/live/DOCUMENTATION/6000/DOC6208/en_US/symcEncrDesktop_103_win_quickstart_en.pdf.

[42] *Microsoft: Encrypting File System (EFS) files appear corrupted when you open them* [online]. 2018 [cit. 2019-05-01]. Dostupné z: https://support.microsoft.com/sk-sk/help/329741/encrypting-file-system-efs-files-appear-corrupted-when-you-open-them.

[43] *Porovnania anitivírusových riešení: Recenzia podnikových produktov na šifrovanie disku* [online]. AV-Comparatives, 2016 [cit. 2019-05-01]. Dostupné z: https://encryption.eset.com/sk/wp-content/uploads/sites/31/2016/08/avc_encryption_eset_201701_sk-2.pdf.

[44] *Microsoft. Windows IT Pro Center: BitLocker Drive Encryption in Windows 7: Frequently Asked Questions: Microsoft Docs* [online]. 2012 [cit. 2019-05-01]. Dostupné z: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-7/ee449438(v=ws.10)#BKMK_DecryptFirst.

[45] *Microsoft*. *Windows IT Pro Center: Download SQL Server Management Studio (SSMS): SQL Docs* [online]. 2019 [cit. 2019-05-01]. Dostupné z: https://docs.microsoft.com/en-us/sql/ssms/download-sql-server-management-studio-ssms?view=sql-server-2017.

[46] ŠEVEČEK Ondřej. *BitColdKit* [online]. 2017 [cit. 2019-05-05]. Dostupné z: https://www.sevecek.com/Files/Forms/AllItems.aspx?RootFolder=%2ffiles%2fBitColdKit&FolderCTID=0x012000CB55F222855F0C49A11DB47971A0FB8E.

ZOZNAM POUŽITÝCH SKRATIEK

3DES	Triple DES
AD	Active Directory
AD DS	Active Directory Domain Services
AES	Advanced Encryption Standard
BIOS	Basic Input Output System
BSOD	Blue Screen of Death
CA	Certification Authority
CBC	Cipher Block Chaining
CSM	Compatibility Support Module
DB	Database
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Naming System
DRA	Data Recovery Agent
DVD	Digital Versatile Disk
EFS	Encrypted File System
IEC	The International Electrotechnical Commission
FDE	Full Disk Encryption
FES	File Encryption System
FIPS	Federal Information Processing Standard
FSMO	Flexible Single Master Operations
FVEK	Full Volume Encryption Key
GPO	Group Policy Object
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISO	ISO 9660 file system
IT	Information Technology
KB	KiloByte
MAC	Message Authenticity Check
MBAM	Microsoft BitLocker Administration and Monitoring
MDOP	Microsoft Desktop Optimization Pack
NTFS	New Technology File System
OID	Object Identifier
OS	Operating System
OU	Organization Unit
PC	Personal Computer
PCR	Platform Configuration Registers
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
PXE	Preboot Execution Environment

ROM	Read Only Memory
RSA	Rivest–Shamir–Adleman
SCCM	System Center Configuration Manager
SED	Self Encryption Drives
SHA	Secure Hash Algorithm
SQL	Structured Query Language
SRK	Storage Root Key
TCG	Trusted Computing Group
TCP/IP	Transmission Control Protocol/Internet Protocol
TPM	Trusted Platform Module
UEFI	Unified Extensible Firmware Interface
USB	Universal Serial Bus
VHD	Virtual HardDrive
VMK	Volume Master Key
WDS	Windows Deployment Services
XOR	Exclusive OR
XTS-AES	XEX - Based Tweaked - Codebook Mode With Ciphertext Stealing - Advanced Encryption Standard

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK