

Universiteti publik Kadri Zeka

Fakulteti i Shkencave Kompjuterike

# Siguria e Internetit

Punim Seminarik

FDE, PCI DSS, BYOE

Mësimdhënësi: Studenti:

Vlera Bllaca

Prof. Ass. Dr. Nysret Demaku

PhD.c. Liridon HOTI

Maj, 2021

Gjilan

# Përmbajtja

[Përmbajtja 2](#_Toc73291635)

[Lista e figurave 3](#_Toc73291636)

[Lista e tabelave 4](#_Toc73291637)

[Hyrje 5](#_Toc73291638)

[Fjalorth 6](#_Toc73291639)

[1. Full Disk Encryption – FDE 7](#_Toc73291640)

[1.1. Karakteristikat dhe avantazhet e FDE-së 9](#_Toc73291641)

[1.1.3. Karakteristikat e FDE-së 9](#_Toc73291642)

[1.1.2. Avantazhet e FDE-së 10](#_Toc73291643)

[1.1.3. Disavantazhet e FDE-së 10](#_Toc73291644)

[1.2. Full Disk Encryption Permissions 11](#_Toc73291645)

[1.3. Gjuhët të cilat i përkrah FDE 12](#_Toc73291646)

[1.4. Full Disk Encryption Software 12](#_Toc73291647)

[2. Payment Card Industry Data Security Standard 14](#_Toc73291648)

[2.1. Historia e PCI 15](#_Toc73291649)

[2.2. Kërkesat e PCI DSS 16](#_Toc73291650)

[2.3. Avantazhet e PCI DSS 21](#_Toc73291651)

[3. Bring Your Own Encryption 22](#_Toc73291652)

[3.1. Sfidat e BYOE 24](#_Toc73291653)

[References 26](#_Toc73291654)

# Lista e figurave

[Figure 1 Full disk encryption 7](#_Toc73291667)

[Figure 2 User account Identification 8](#_Toc73291668)

[Figure 3 FDE 9](#_Toc73291669)

[Figure 4 FDE Software 13](#_Toc73291670)

[Figure 5 PCI DSS 14](#_Toc73291671)

[Figure 6 Ekosistemi i PCI pagesave 15](#_Toc73291672)

[Figure 7 PCI DSS app 16](#_Toc73291673)

[Figure 8 Kerkesat e PCI 17](#_Toc73291674)

[Figure 9 PCI DSS Compliance Life Cycle 21](#_Toc73291675)

[Figure 10 Arkitektura e BYOE 22](#_Toc73291676)

[Figure 11 Arkitektura e BYOK 23](#_Toc73291677)

[Figure 12 Arkitektura e CYOE 24](#_Toc73291678)

# Lista e tabelave

[Table 1 Full Disk Encryption Permissions 11](#_Toc73291679)

[Table 2 Informacionet e kartes 19](#_Toc73291680)

[Table 3 Informatat e transaksionit 20](#_Toc73291681)

# Hyrje

Në këtë punim seminarik do shtjellohen disa tema, siq janë: FDE – Full Disk Encryption, PCI DSS – Payment Card Industry Data Security Standard dhe BYOE – Bring Your Own Encryption. Do tregohet se qka janë këto në sigurinë e internetit dhe se si ndikojnë në jetët tona. Gjithashtu do tregohen avantazhet, disavantazhet, rëndësia e tyre, dhe shumë punë të cilat na mundësojnë këto tri encryptions t’i realizojmë.

# Fjalorth

FDE – Full Disk Encryption

PCI DSS - Payment Card Industry Data Security Standard

BYOE – Bring yosiqur own Encryption

BYOD – Bring your own Device

CYOE – Choose your own Encryption

HSM – Hardware security Model

R – Read

W – Write

L – List

X – Execute

M – Modify

D – Delete

F – Full Control

C – Create

Transit – Data in motion

# Full Disk Encryption – FDE

Kur flasim për enkriptimin këto ditë, përqendrohemi tek sigurimi i gjërave si konektimi me internet, fjalëkalimet në ndonjë server diku dhe është një frikë se do aksesohen nga ndonjë person tjetër pasi që të gjitha të dhënat të cilat janë me vlerë për ne gjenden online. Por le të themi se keni bërë të pamundurën për t’i fshehur gjërat tuaja duke e vendosur një fjalëkalim me shumë karaktere për rrjetet sociale, apo edhe diku tjetër, qka nëse pas të gjitha këtyre një person hyn fshehurazi në shtëpi dhe merr llaptopin, kompjuterin ose harddiskun tuaj dhe fillon që të kontrolloj të dhënat tuaja në llogaritë e ndryshme të cilat i keni lënë hapur në pajisjen tuaj.

Zgjidhja e këtij problemi është Full Disk Encryption ose Whole Disk Encryption ku me anë të këtij enkriptimi, i gjithë disku ose drive-i enkriptohet dhe në këtë mënyrë njeriu i cili ka në dorë pajisjen tuaj që ka hyrë në shtëpi pa leje, nuk mund të kyqet në të dhënat tuaja personale kështu që kur e startoni kompjuterin(boot) apo pajisjen tuaj, do ju paraqitet që të shkruani një qelës enkriptimi, pra ndonjë fjalëkalim.

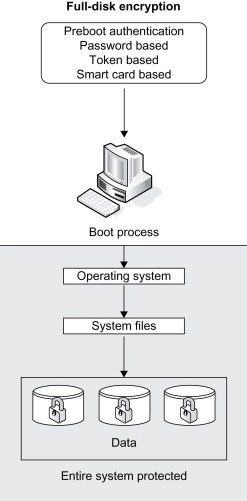


Figure 1 Full disk encryption

Sapo të shkruani qelësin e duhur, atëherë do dekriptohet disku dhe ju mund t’i qaseni të dhënave apo fajllave të cilat i keni pasur të ruajtur në pajisje. Por nëse fjalëkalimi të cilin e keni lënë si qelës të enkriptimit të diskut, nuk është edhe shumë i fortë (nuk ka shkronja të mëdha, të vogla, numra, simbole, ndonjë emër familjari apo ditëlindje) atëherë do jetë më e lehtë që të thyhet ky qelës nga personi i cili tenton që të kyqet në pajisjen tuaj. Pra, me enkriptimin e plotë të diskut (FDE) parandalohet rrjedhja e të dhënave përmes humbjes së një laptopi ose një hard drive-i. Të gjithë përdoruesit e pa autorizuar nuk mund të lexojnë të dhënat tuaja apo ta startojnë pajisjen.



Figure 2 User account Identification

## **. Karakteristikat dhe avantazhet e FDE-së**

### **Karakteristikat e FDE-së**

Full disk encryption ofron funksionet e mëposhtme të sigurisë:

* Strong user authentication.
* Mbështetje për identifikimin e përdoruesit duke përdorur dynamic tokens.
* Secure Remote Help për përdoruesit të cilët kanë harruar fjalëkalimin.
* Konfigurimi dhe administrimi qendrorë.
* Bllokimin e tastierës dhe ruajtjen e ekranit (screen saver).
* Numër i limituar të shkruajtjes së fjalëkalimit apo të username-it gabim.
* Ruajtja e kyqjeve të suksesshme apo tentimeve të dështuara të kyqjes.

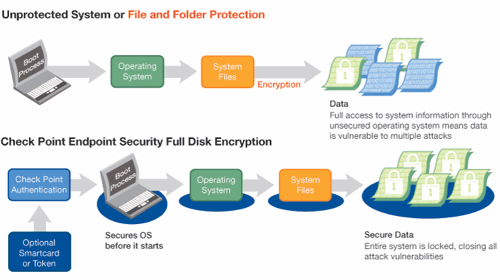


Figure 3 FDE

### **1.1.2. Avantazhet e FDE-së**

Si administratorë i plotë të kriptimit të diskut, ju keni kontroll të centralizuar të një sistemi të decentralizuar ku ju mund të kryeni:

* Instalimin, modifikimin dhe heqjen e FDE-së në kompjuterët e përdoruesve në rrjet.
* Konfigurimin dhe vendosjen e sigurisë dhe politikave në kompjuterët e përdoruesve, përdorë algoritme të forta të kriptimit për të kriptuar disqet në PC tuaj. Të dhënat janë të pa arritshme nëse nuk keni një qelës të saktë.
* Modifikimin e cilësive të politikës së sigurisë për t’iu përshtatur nevojave të të gjithë popullsisë së përdoruesve të grupeve të zgjedhura të përdoruesve ose përdoruesve individual.
* Administrimi ditorë i sistemit.
* Enkriptimi automatik i të dhënave, FDE enkripton të dhënat sa më shpejt që pastaj ato të ruhen në harddisk si dhe shmangen gabimet gjatë enkriptimit me enkriptimin automatik të të dhënave.

### **1.1.3. Disavantazhet e FDE-së**

* Nuk mbron datat kur janë bë Transit, megjithatë kriptimi i plotë i diskut ka të metat e veta, nëse jeni duke shpërndarë të dhëna ndërmjet pajisjeve ose përmes postës, atëherë ato të dhëna nuk mbrohen dhe mund të hakohen shumë lehtë.
* Ngadalëson kompjuterin, kur përdorim full disk encryption i tërë disku është i koduar. Në këtë rast, qdo herë kur përpiqemi të lexojmë të dhënat e diskut, kërkohet qelësi që të të lejojë akses në të dhëna dhe ky proces e ngadalson kompjuterin.
* Riparimi i komplikuar i të dhënave, enkriptimi e ka një të metë që e bënë të vështirë rikuperimin e të dhënave por kjo gjë është normale pasi që nëse nuk do ishte i vështirë rikuperimi atëherë qfarë kuptimi do kishte enkriptimi?

## **Full Disk Encryption Permissions**

Kjo tabelë përshkruan lejet që kërkon Full Disk Encryption:

R-Read,

W-Write,

L-List,

X-Execute,

M-Modify,

D-Delete,

F-Full Control,

C-Create

Një vijë (-) – Not Applicable.



Table Full Disk Encryption Permissions

*Instalimi -* Instalimi i korrespondon performimit të instalimit të Full Disk Encryption. Trajtohet nga Agjenti i pajisjes dhe nuk duhet leje speciale për instalimin e FDE.

*Heqja -* Heqja i korrespondon heqjes së aplikacionit të Full Disk Encryption nga Windowsi te pjesa e Add/Remove Programs. Për performimin e kësaj duhet që përdoruesi të jetë i kyqur si administratorë, pra të ketë lejet e administratorit në Windows.

*Tray(Px2) –* i korrespondon fajllit CPTray.exe, që përdor dyekzekutues kur kryen punë.

*PS Control –* i korrespondon punëve të cilat kryhen prej ekzekutuesit pscontrol.

## **Gjuhët të cilat i përkrah FDE**

* Portugalisht (Brazil)
* Frengjisht(Kanada)
* Kinezisht (E thjeshtesuar)
* Kinezisht (Taiwan)
* Qeke
* Angleze
* Frenge
* Gjermane
* Hungareze
* Italiane
* Japoneze
* Polish
* Portuguese
* Rusisht
* Spanjollisht
* Thai

## **Full Disk Encryption Software**

Për të zgjedhur një Software i cili e enkripton të gjithë diskun tuaj atë herë duhet t’i keni parasyshë disa gjëra:

* Sistemin operativ – Microsoft dhe Apple të dyja kanë enkriptimin e tyre të plotë që mund të jetë e mjaftueshme për disa raste.
* Menaxhimi – Sa lehtë apo sa vështirë është që të menaxhojmë apo të rikthejmë qelësat e enkriptimit
* Vlera dhe hargjimet – kur vie puna për full disk encryption nuk justifikohet shuma se sa shpenzojmë për të.

*Disa software si FDE:*

* Apple FileFault
* Check Point
* Eset Endpoint Encryption Pro
* McAfee Complete Data Protection
* Micro Focus ZENworks Full Disk Encryption
* Microsoft BitLocker
* R&S Trusted Disk
* Sophos SafeGuard Encryption
* Symantec
* TrendMicro

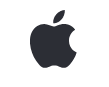


Figure 4 FDE Software

# Payment Card Industry Data Security Standard

Standardi i sigurisë së të dhënave të industrisë së kartave dhe të pagesave (PCI DSS) standard që u krijua me qëllim që të rriten kontrollet rreth të dhënave të mbajtësve të kartave dhe që të zvogëlohen mashtrimet me karta të kreditit. PCI DSS është cila do organizatë e cila pranon pagesa nga kartelat, ruan, proceson dhe transmeton debit ose credit të dhëna që janë në pajtueshmëri me PCI DSS.

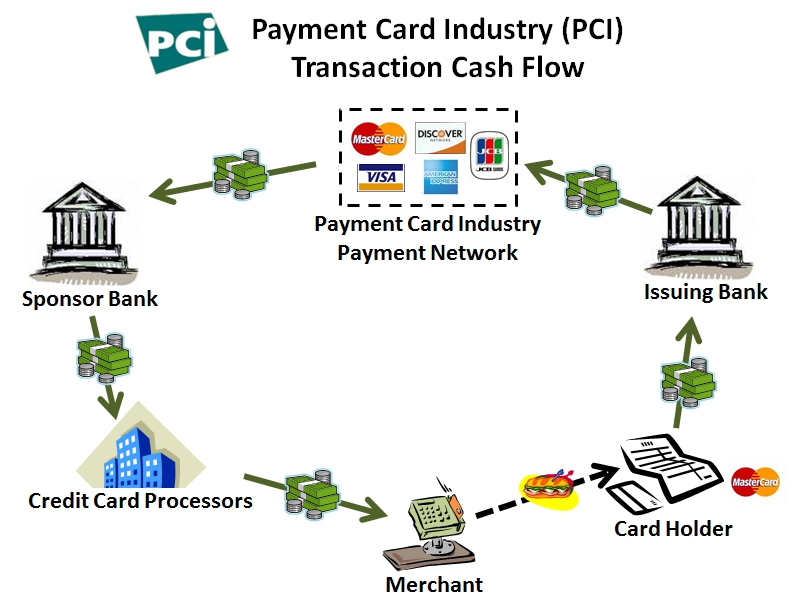


Figure 5 PCI DSS

Në figurën 6 shihen entitetet në pagesat me kartelë që janë:

* Mbajtësi i kartelës, presoni që mban kartelën,
* Shitësi që shet dhe pranon kartela,
* Service provider që i siguron të gjitha shërbimet e pagesave për shitësin,
* Acquiring bank që konekton një kartelë për pagesë dhe ka një kontratë për pagesa me kartelë me shitësin,
* Issues bank, lëshon kartela të cilat pastaj ata që marin kartelat bëhen mbajtës të kartelës, Card brand që është një ekosistem I pagesave që thirret “association network” me procesorët e vet siq janë Visa, MasterCard, Amex etj.

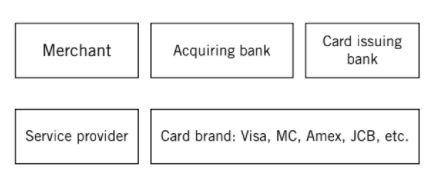


Figure 6 Ekosistemi i PCI pagesave

## **2.1. Historia e PCI**

PCI DSS ka evoluar gjatë viteve, duke filluar nga vitet 1990 ku brendet e kartelave kishin zhvilluar standarde të ndryshme që i bëjnë më të sigurtë informacionet sensitive, Në rastin e Visa-s regjionet e ndryshme krijuan standarde të ndryshme pasi që vendet Evropiane dhe Kanadaja kishin standarde të ndryshme duke u krahasuar me US.

VISA USA kishte filluar e para në vitin 2001, ku kishte lëshuar një mbajtës të Cardholder Information Security Program (CISP). Ky CISP ishte versioni fillestar i PCI DSS pastaj me zhvillimin e pa ndalur ishte krijuar versioni 2.3 në mars të vitit 2004, gjatë kësaj kohe Visa ishte duke bashkëpunuar me MasterCard, këto procedura auditimi vazhduan të rriteshin dhe të evulonin duke trajtuar tema të ndryshme që ishin të ndjeshme për të dhënat që gjendeshin në kartelë. Kishte përpjekje të ndryshme për sigurinë e kartelave por kishte mospërputhje të programeve të ndryshme.



Figure 7 PCI DSS app

## **Kërkesat e PCI DSS**

Secili version i PCI DSS ka 6 kërkesa të nivelit të lartë të cilat nuk kanë ndryshuar edhe pse janë krijuar versione tjera të PCI DSS. Secia kërkesë/nënkërkesë shtjellohet në tre seksione.

*Deklarata e kërkesës* - Kjo deklaratë e përcakton përshkrimin e kërkesës.

*Proceset e testimit* – Proceset dhe metologjitë e kryera nga vlerësuesi për konfirmimin e zbatimit të duhur.

*Udhëzimi* – Shpjegon qëllimin kryesorë të kërkesës dhe përmbajtjen e kërkesës.

Kërkesat:

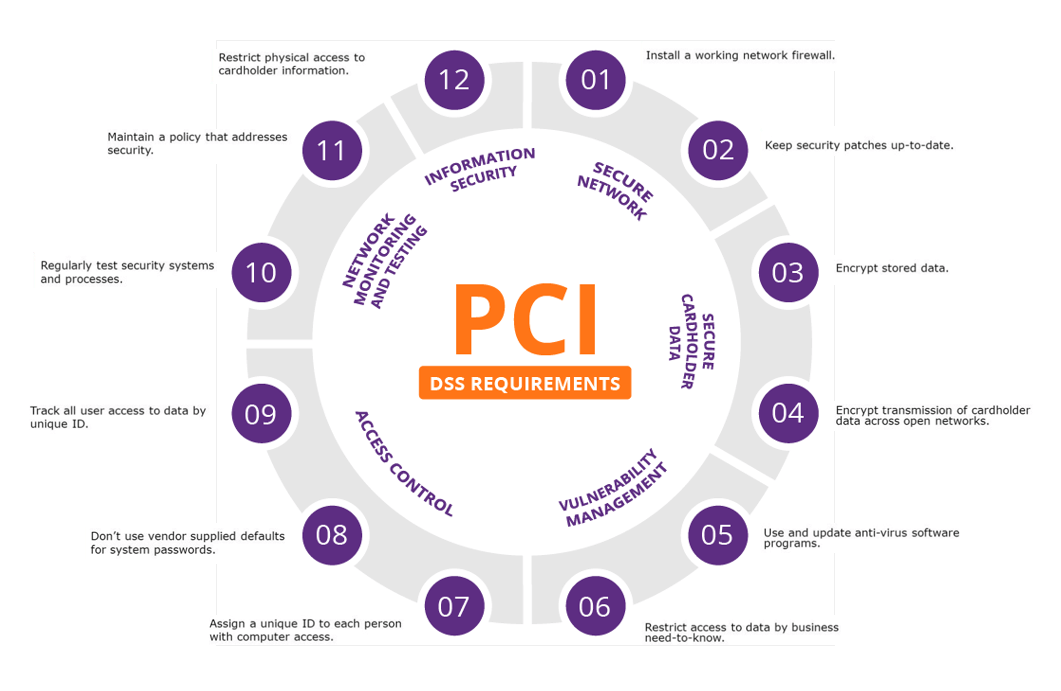


Figure 8 Kerkesat e PCI

Instalimi dhe mirëmbajtja e një konfigurimi të firewall për të mbrojtur të dhënat e mbajtësit të kartelës. Qëllimi i një firewall është të skanojë të gjithë trafikun e rrjetit, të bllokojë hyrjen në sistem të rrjeteve të pasigurta.

Ndryshimi i parazgjedhjeve të furnizuesit për fjalëkalimet e sistemit dhe parametrat e tjerë të sigurisë. Këto fjalime zbulohen lehtësisht përmes informacionit publik dhe mund të përdoren nga individë me qëllim të keq për të fituar akses të pa autorizuar në sisteme.

Mbrojtja e sistemeve nga malware dhe kryerja e azhurnimeve të rregullta të softuerit anti-virus. Malware mund të hyjë në një rrjet përmes mënyrave të shumta, duke përfshirë përdorimin e internetit, pajisjet mobile etj.

Kufizimi i aksesit në të dhënat e mbajtësit të kartelës vetëm për personelin e autorizuar. Sistemet dhe proceset duhet të përdoren për të kufizuar hyrjen në të dhënat e mbajtësve të kartave mbi bazën e “nevojës për të ditur”.

Identifikimi i aksesit fizik. Qdo personi me qasje në përbërësit e sistemit duhet të caktohet një identifikim unik ID që lejon përgjegjësinë e qasjes në sistemet kritike të të dhënave.

Kufizimi i aksesit fizik në të dhënat e mbajtësit të kartelës. Aksesi fizik në të dhënat e mbajtësit të kartelës ose sistemet që i mbajnë këto të dhëna duhet të jenë të sigurta për të parandaluar hyrjen ose heqjen e paautorizuar të të dhënave.

Ndjekja dhe monitorimit i gjithë akseist në të dhënat em bajtësit të kartelës dhe burimeev t rrjetit. Duhet të ekzistojnë mekanizmat e regjistrimit për të gjurmuar aktivitetet e përdoruesve që janë kritike për të parandaluar, zbuluar ose minimizuar ndikimin e kompromiseve të të dhënave.

Testimi i sistemeve dhe proceseve të sigurisë rregullisht. Dobësitë e reja zbulohen vazhdimisht. Sistemet, proceset dhe softueri duhet të testohen shpesh për të zbuluar dobësitë që mund të përdoren nga individë me qëllim të keq.

Mbajtja e një politike të sigurisë së informacionit për të gjithë personalein. Njëpolitikë e fortë sigurie përfshinë përbërjen e personelit për të kuptuar ndjeshmërinëe të dhënave dhe përgjegjësinë e tyre për t’i mbrojtur ato.

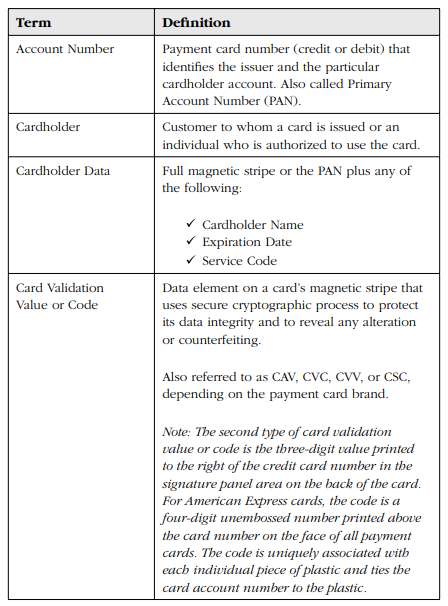


Table 2 Informacionet e kartes

Më poshtë janë paraqitur informacionet se kur bëhet një transaksion.

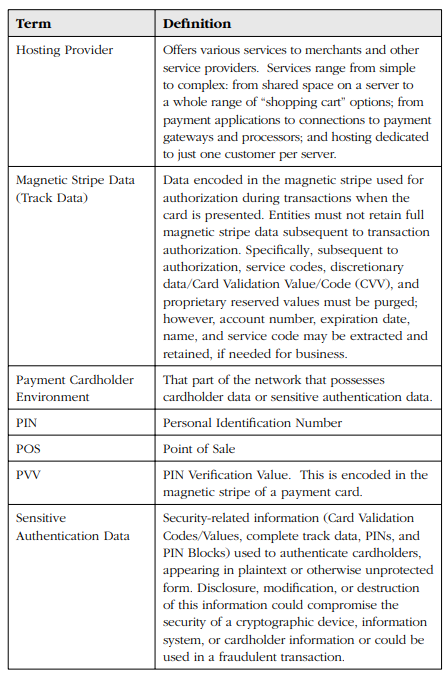


Table 3 Informatat e transaksionit

# Avantazhet e PCI DSS

*Redukton rrezikun e shkeljes së të dhënave*, sepse ruan të gjitha informacionet dhe bëhet më e vështirë që këto të thyhen si dhe zvogëlohet edhe sasia e e të dhënave të ndjeshme të cilat mund t’i vjedhin.

*Mbronë konsumatorët,* kurrë nuk është kërkuar më shumë privatësia e ndonjë personi më shumë se sa në bankë, të gjithë kanë eksperienca të ndryshme me privatësinë e tyre kshtu që me mbrojtjen e saj nga bankat e ndryshme për akontet e tyre, kjo i jep siguri dhe besnikëri klientëve duke referuar ata familjarë e miq për shfrytëzimin e shërbimeve tuaja.

*E rrit reputacionin e brendit,* kur ka më pak hakim apo vjedhje të të dhënave atëherë kjo do të thotë që më shumë njerëz përdorin këtë sistem dhe lë përshtypje të mira nga ta.

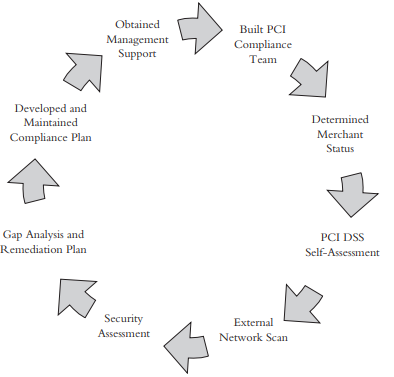


Figure 9 PCI DSS Compliance Life Cycle

# Bring Your Own Encryption

BYOE (sillni qelësin tuaj) i referohet një modeli të të sigurisë së llogaritjes së re që synon të ndihmojë klientët e cloud services të përdorin programin e tyre të kriptimit në mënyrë që të krijojnë qelësin e tyre personal të kriptimit dhe të kenë kontrollë të plotë në gjërat e tyre apo pajisjet e tyre personale.

Ky lloj i enkriptimit u propozua në mënyrë që t’i siguronte pronarit të të dhënave kontrollë të plotë dhe siguri. Ky encryption sigurohet që edhe klientit t’i pëlqejë encryption key që i gjenerohet, pra ka një balancë mes sigurisë dhe efikasitetit.

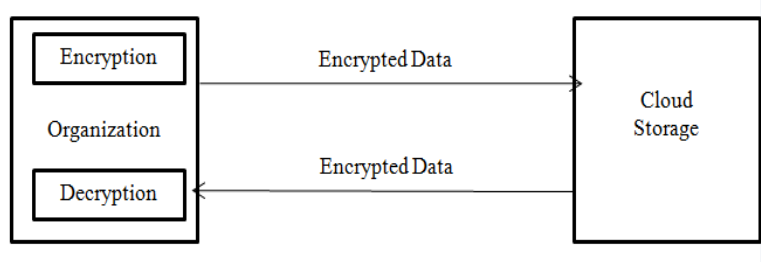


Figure 10 Arkitektura e BYOE

Krahasuar me zgjidhjet të cilat janë të enkriptimit që gjenden në cloud providers, BYOE jep më shumë besim në mbrojtjen e të dhënave dhe ju mundëson juve që të keni:

* Performancë të lartë të enkriptmit AES të përmirsuar nga përshpejtimi i harduerit dhe politikat e kontrollit të hollësishëm, duke përfshirë privilegjin e kontrollit të hyrjes së përdoruesit. BYOE kontrollon kush, përmes të cilit proces dhe në kohë të përcaktuar mund të shoh të dhëna specifike.
* Arkitekturë që siguron skedarë të pastrukturuar, baza të të dhënave të strukturuara dhe mjedise të të dhënave të mëdha dhe ju lejon të migroni të dhëna midis mjediseve cloud dhe serverave të brendshëm pa kohën dhe koston e deshifrimit. Për kontrolle shtesë të rëndësishme dhe përmbushje të një gjerësie më të gjerë të rregulloreve, shtoni lehtësisht ruajtjen e formatit ose kriptimin ose tokenizimin tradicional të aplikacioneve duke përdorur RESTful API ose biliotekat më të fuqishme dhe të sigurta të kriptimit të industrisë.
* Zgjerimet e BYOE mundësojnë përdorimin e të dhënave gjatë operacioneve të kriptimit dhe re-qelësave (rekeying) me Transformimin e të dhënave Live, për të izoluar dhe siguruar ambiente kontenjerësh duke krijuar zona kriptimi të bazuara në politikë. BYOE monitoron dhe regjistron aksesin e skedarit për të përshpejtuar zbulimin e kërcënimit dhe integrimin e Regjistrit të inteligjencës së sigurisë me mjetët e njohura SIEM.
* Menaxhimi i thjeshtuar i qelësit në vendosjet brenda dhe në multi-cloud duke centralizuar kontrollin në Cipher Trust Manager.

Krahasojmë skemat e BYOK, CYOE pastaj krahasojmë me BYOE:

*BYOK:*

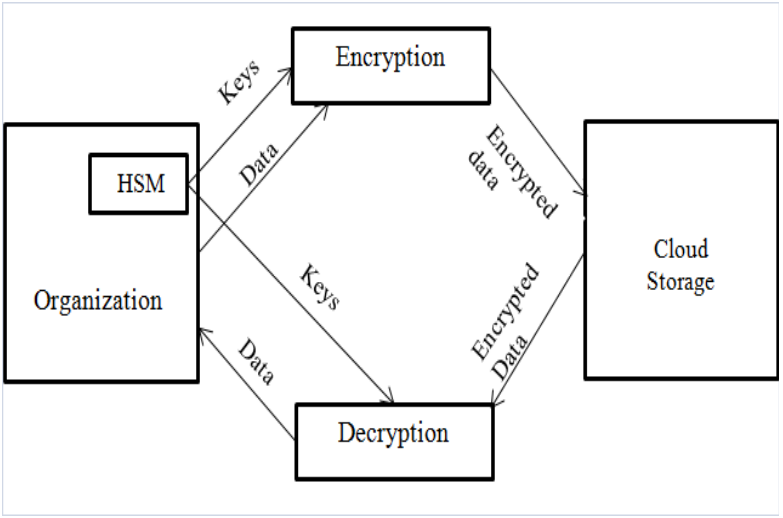


Figure 11 Arkitektura e BYOK

Shohim në figurën 11 se organizata ka një Hardware security Module(HSM) dhe pastaj përdorë disa qelësa që i enkriptojnë të dhënat dhe pastaj ruhen ato të dhëna në Cloud Storage. Kur dëshirojnë të dekriptohen ato pastaj kthehen te organizata se ku është filluar.

*CYOE:*

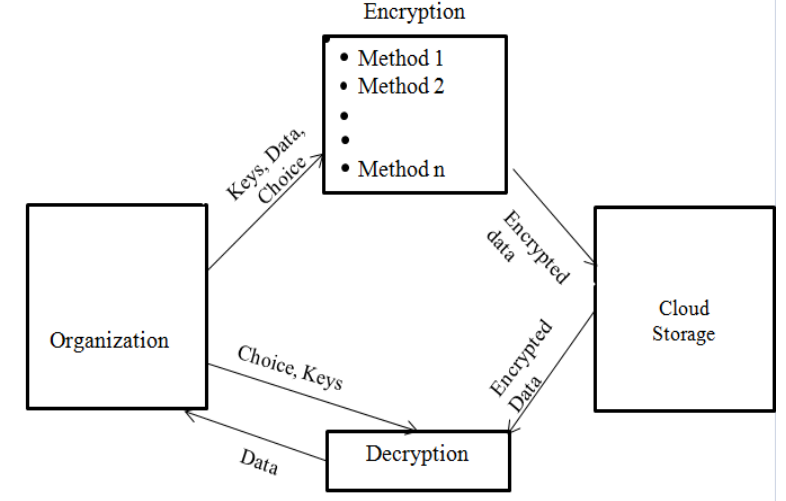


Figure 12 Arkitektura e CYOE

Shohim në figurën 12 se nga organizata me anë të qelësave dhe mundësive të zgjedhjes së metodave prej 1 deri në n ato enkriptohen pastaj ruhen në Cloud Storage dhe nëse dëshirojmë t’i dekriptojmë të dhënat atëherë përmes qelësave dhe mundësive të zgjedhjes së metodave atëher mund të kthehen të gjithë fajllat siq kanë qenë në fillim.

## **3.1. Sfidat e BYOE**

BYOE si shumë teknologji të tjera nuk mund të vijë pa asnjë kosto. Megjithëse koncepti i BYOE ka lindur për të parandaluar ndërmarrjet nga cloud për shkak të qështjeve të sigurisë, kërkohet një motivim më i fortë për t’i bërë ndërmarrjet të pranojnë BYOE për shkak të sfidave në lidhje me zbatimin e tij.

* *Outsourcing data processing*

Sfida më e madhe vjen nga aplikacionet SaaS të cilat një ndërmarrje synon t’i transferojë të dhënat e saj, SaaS ofruesit nuk kanë zbatuar ende teknologjitë për klientët që të mbajnë qelësat e tyre dhe të kenë një funksionalitet të plotë. Kriptosistemi që ndërmarrja duhet të mbajë në cloud do të sjellë disa kosto për organizatën.

* *Length of keys*

Vendosja e qelësave të gjatë zakonisht është për të pasur një siguri më të madhe. Një organizatë që përdor një sistem të enkriptimit të tyre mund të kalojnë aq kohë sa është e mundur pa e ndërruar qelësin. Por kjo do thotë që do konsumohet kujtesa dhe do ketë një proces të ngadalshëm kriptografik.

* *Economic issues*

Barrierat ekonomike nga ndërmarrjet janë një sfidë, ndërrmarrjet e vogla me burime të limituara janë përdorues të rregullt të cloud service-s.

* *Loss of keys*

Në rast se HSM qelësat e ruajtur humben dhe nuk ka mundësi që t’i rikthejmë atëherë këto qelësa janë të humbur, qelësat janë të transferuar direkt nga ndërmarrja HSM tek HSM cloud dhe nuk shihen kurrë në cloud service dhe për këtë arsye kurr nuk mund t’i kthejmë më.

# References

|  |  |
| --- | --- |
| [1] | A. C. Brenden R. Williams, PCI Compliance: Understand and Implement Effective PCI Data Security Standard Compliance, 2007. |
| [2] | T. M. Virtute, Payment Card Industry Data Security Standard Handbook, New Jersey: John Wiley & Sons, Inc. Hoboken, 2008. |
| [3] | "Thales," 2021. [Online]. Available: https://cpl.thalesgroup.com/encryption/bring-your-own-encryption. [Accessed 2021]. |
| [4] | "How Does Full Disk Encryption Work," Techquckie, 2016. [Online]. Available: https://www.youtube.com/watch?v=UPW1Hqvx6zo&ab\_channel=Techquickie. [Accessed 2021]. |
| [5] | "TechTarget," TechTarget Contributor, 2014. [Online]. Available: https://whatis.techtarget.com/definition/full-disk-encryption-FDE. [Accessed 2021]. |
| [6] | I. S. Vishnu Kumar, "Bring-Your-Own-Encryption: How Far Are We?," in *11th International Conference on Industrial and Information System (ICIIS)*, 2016. |