Enkripcijske tehnologije u modernim Windows baziranim informacionim sistemima

Damir Dizdarević
Logosoft d.o.o.
Sarajevo, BiH
ddamir@logosoft.ba

Sažetak—**Zaštita podataka u digitalnom obliku uvijek je aktuelna tema. Ipak, pristup zaštiti podataka u slučajevima kada je njihova lokacija unaprijed poznata je drugačiji od onoga kada lokaciju podataka nismo u mogućnosti precizno definisati. Konzumerizacija IT-a, omasovaljavanje upotrebe različitih uređaja, kao i svojevrsna revolucija u razumijevanju IT-a generalno, koja se najviše ogleda u sveprisutnosti cloud tehnologija, trendovi su koji značajno mijenjaju i pogled na zaštitu podataka. Podaci se danas nalaze na mnogo različitih lokacija i različitih uređaja, od kojih je veliki broj njih neupravljiv i nekontrolisan od strane korporativnog IT-a. Ovaj rad se bavi nekim ključnim tehnologijama za zaštitu podataka koje su danas aktuelne, kao i pristupima za zaštitu podataka u zavisnosti od scenarija njihove upotrebe i lokacije. Iako se rad referira na neke konkretne tehnologije u Windows okruženjima, pogrešno bi ga bilo smatrati orijentisanim isključivo na tu platformu. Operativni sistem Windows jeste dominantan u laptop/desktop segmentu, no u području uređaja u širem smislu to nije slučaj, pa ćemo stoga i tehnologije razmatrati multiplatformski gdje god je to moguće.**

Ključne riječi- enkripcija, zaštita, kriptovanje, EFS, Bitlocker, Rights management

I. UVOD

Istraživanja analitičarskih kuća, poput Gartnera i Forrestera, pokazuju da više od polovine današnjih uposlenika globalno, pošalje svoj prvi email prije nego dođe na posao, a da gotovo dvije trećine njih pošalje svoj posljednji mail (tokom dana), nakon što napusti radno mjesto. Ovo vrlo paradigmatično pokazuje da je definicija radnog mjesta danas vrlo fleksibilna, te da je radno mjesto mobilno više nego ikada prije. Zajedno sa radnim mjestom, i podaci postaju mobilni, jer su i uređaji na kojima se oni generišu ili konzumiraju vrlo mobilni. Slična istraživanja pokazuju da veliki broj uposlenika drži manju ili veću količinu poslovnih podataka na nekom od privatnih cloud-baziranih storage servisa (npr. OneDrive, Dropbox, Google Drive i sl.). Ova činjenica je posljedica ranije opisane mobilnosti radnog mjesta. Umjesto nekadašnjeg snimanja podataka na USB stick-ove, danas je mnogo lakše ono na čemu se radi pohraniti na svoj privatni cloud storage servis, te imati pristup tim podacima sa bilo kojeg mjesta i bilo kojeg uređaja. To omogućava da se, pored posjedovanja zaštitne kopije podatka, posao koji je započet na jednom mjestu može završiti na drugom mjestu ili obrnuto. Interesantno je ipak da je u većini poslovnih okruženja ovakva praksa uspostavljena od strane krajnjih korisnika, bez prethodne aktivnosti kompanijskog IT-a.

Zbog svega ovoga, poslovni podaci gotovo svake današnje tipične kompanije u BiH ili bilo gdje u regiji, uglavnom su, moglo bi se reći, disperzirani između storage sistema same kompanije, računara krajnjih korisnika, te privatnih cloud storage servisa.

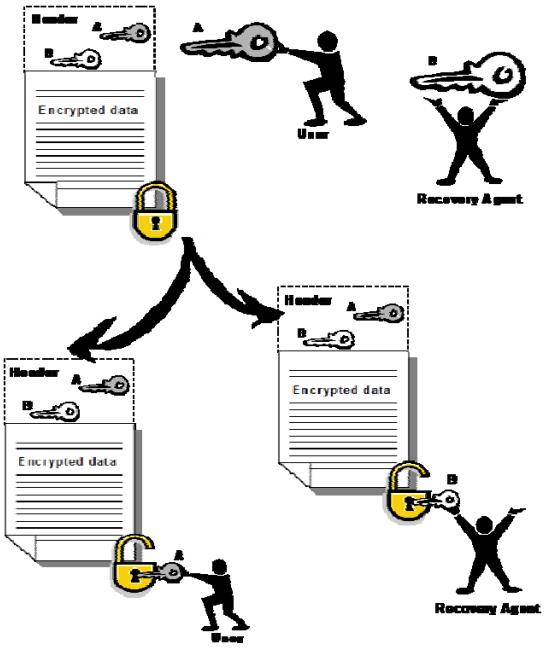
Promjena načina posmatranja poslovnih podataka, kao i tehnika za njihovu zaštitu ključna je promjena koju današnji IT ljudi i odjeli moraju da naprave. Izostanak te promjene i držanje pri starim tehnikama može samo umanjiti funkcionalnost, a neće povećati sigurnost ni u kom pogledu. Ipak, poznavanje tehnologija koje su korištene ili se i danas koriste za zaštitu tzv. podataka fiksne lokacije, korisno je za razumijevanje kako same tehnologije tako i današnjih potreba odnosno manjkavosti ranijih pristupa.

II. TEHNOLOGIJE ZA ENKRIPCIJU NA NIVOU FAJLA (PRIMJER – EFS)

Tehnologije zaštite podataka njihovom enkripcijom poznate su još odavno. Većina tih tehnologija, bez obzira na proizvođača, radila je, i danas radi, na relativno klasičnom principu. Pri pokretanju procesa kriptovanja, generisao bi se simetrični ključ za kriptovanje podataka, koji bi se potom koristio u algoritmu poput DES-a, 3DES-a, AES-a (kasnije i jačih) da se sadržaj kriptuje, odnosno učini nečitljivim bez posjedovanja ključa, koji bi ga reverznim procesom ponovo učinio čitljivim i upotrebljivim. U slučaju Encrypting File System (EFS) tehnologije, taj simetrični ključ bi se potom kriptovao kroz asimetrični algoritam odnosno algoritam koji koristi asimetrične ključeve – privatni i javni. Ova dva ključa (često nazvana „par ključeva“ ili eng. „key pair“) funkcionišu na način da ono što javni ključ kriptuje, samo privatni može da dekriptuje i obrnuto. Pored toga, za svaki par privatnog i javnog ključa sa ovim osobinama, ne postoji treći ključ, koji je sa bilo kojim od ova dva u istoj relaciji. Time se praktično svaki par ključeva čini unikatnim i uvijek vezanim za identitet korisnika (ponekad i servisa koji ih koristi). U Windows okruženjima, ovaj par ključeva se jedinstveno generiše za svakog korisnika, te pohranjuje uz korisnički digitalni certifikat (izdat na lokalnom računaru ili od strane Certificate Authority servera). Na ovaj način, korisnik je uz posjedovanje ličnog

digitalnog certifikata mogao da raspolaže i svojim parom ključeva. Do korisničkog javnog ključa mogao je da dođe svako kome bi korisnik distribuirao svoj javni dio certifikata (zapravo i javni ključ), dok je privatni ključ uvijek dostupan samo i isključivo korisniku kojem je certifikat izdat. Ovaj princip, korištenja asimetričnog para ključeva, koristi se i u tehnologiji digitalnih potpisa, kao metod dokazivanja identiteta odnosno nepromijenjivosti sadržaja, ali to je izvan opsega teme ovog rada.

Vratimo li se sad na sam proces kriptovanja, možemo sumirati da su se podaci kriptovali na sljedeći način : Korisnik bi prvo izdao naredbu za kriptovanje fajla kroz komandnu liniju odnosno grafički interfejs. U tom momentu bi se, ukoliko to ranije već nije urađeno, generisao korisnički certifikat (sa namjenom za EFS) te bi se generisao i par ključeva (privatni i javni) za tog korisnika. U sljedećem koraku bi se generisao simetrični ključ za kriptovanje samih podataka. Ovaj ključ bi se iskoristio da se kriptuje sam sadržaj, a potom bi se simetrični ključ kriptovao javnim ključem korisnika, koji je izdao naredbu za kriptovanje podataka. Time je, pored samih podataka i ključ bio osiguran. Tako kriptovan simetrični ključ bi se smjestio u posebno polje u headeru samog kriptovanog fajla.



Slika 1. Koncept rada EFS tehnologije

Pri dekriptovanju podataka, korisnik bi iskoristio svoj privatni ključ da dekriptuje simetrični ključ, a potom bi se simetrični ključ iskoristio za dekriptovanje samog fajla. Logično bi bilo da, manje upućeni čitalac, postavi sebi relativno razumno pitanje : „zašto nam uopšte treba simetrični ključ?“. Zašto jednostavno podatke, odnosno sam fajl, ne zaključamo sa javnim ključem korisnika i time osiguramo da se mogu otključati samo njegovim privatnim ključem. Više je razloga za takav pristup. Kao prvo, algoritmi koji koriste asimetrični pristup po pitanju ključeva (što znači da se ne koristi isti ključ i za kriptovanje i za dekriptovanje) su vrlo neefikasni za veće količine podataka. Zato ih koristimo da bi kriptovali samo simetrični ključ, koji sam po sebi nije naročito velik podatak (uglavnom 128 ili 256 bita). Drugo, svaki korisnik ima jedinstven par privatnog i javnog ključa. Ako ne bismo koristili simetrični ključ, praktično bismo isti par ključeva koristili za sve što se kriptuje umjesto da se novi, jedinstveni simetrični ključ, generiše pri svakom kriptovanju.

Ovakav pristup, dosta dugo je bio jedan od primarnih načina zaštite na nivou fajla u Windows okruženjima, jer mu je sigurnost na dosta visokom nivou, ali je vremenom postao dosta nepraktičan iz nekoliko razloga. Naime, pristup kriptovanim podacima uvijek zahtijeva posjedovanje certifikata i to sa privatnim ključem. Kako se certifikat i privatni ključ pohranjuju unutar korisničkog profila i nisu mobilni (izuzev kada je uključen credential roaming a i tada ograničeno), to je mobilnost samih kriptovanih podataka dosta ograničena. Ukoliko bi se primjerice podatke kriptovane EFS-om htjelo koristiti na drugom računaru, bilo je potrebno uraditi eksport certifikata zajedno sa privatnim ključem (u tzv. *.pfx formatu) te taj isti certifikat importovati na računar na kojem se podaci žele koristiti. Za dosta korisnika, ovo nije trivijalna operacija, posebno uzme li se u obzir da se danas dobar dio fajlova otvara na mobilnim uređajima i tabletima, gdje je dekripcija i manipulacija certifikatima i ključevima, još složeniji posao. Dalje, dijeljenje ovako kriptovanih fajlova sa drugim korisnicima zahtijevalo je da onaj ko je originalno kriptovao fajl bude u posjedu javnog ključa drugog korisnika koji želi koristiti isti fajl. Drugi korisnik mora da eksportuje svoj lični certifikat ali samo sa javnim ključem (u tzv. *.cer formatu) te da ga proslijedi korisniku koji kriptuje fajl. Tada bi korisnik koji kriptuje fajl, nakon generisanja simetričnog ključa i kriptovanja fajla, taj simetrični ključ jednom kriptovao svojim javnim ključem, i smještao u header fajla, a zatim još jednom ponovio tu operaciju sa javnim ključem drugog korisnika, te ponovo smjestio kriptovani ključ u header fajla. Na ovaj način postiže se to da se sada simetrični ključ za otključavanje fajla može otključati i sa privatnim ključem vlasnika fajla, ali i sa privatnim ključem onoga sa kim taj korisnik fajl želi dijeliti. Interesantno je da se ovaj isti metod koristi i kao zaštitni (recovery) mehanizam za ovu tehnologiju. Organizacija koja želi da koristi EFS kao metod zaštite svojih kritičnih podataka, definiše ulogu Recovery agenta čijim se javnim ključem potom zaključava i svaki simetrični ključ za kriptovanje fajlova koji se generiše unutar organizacije. Na taj se način postiže da osoba kojoj je dedicirana Recovery agent uloga može da dekriptuje sve što drugi korisnici kriptuju u slučaju da originalni autor nije u stanju da otključa fajl, iz bilo kojeg razloga.

Međutim, praktični primjeri iz prakse pokazuju da je ovaj pristup i dalje dosta kompleksan i što je još važnije podložan greškama u implementaciji, koje uglavnom rezultiraju gubljenjem pristupa podacima. U svojoj dosadašnjoj praksi autor ovog rada se susreo sa nekoliko tipova loše implementacije enkripcijskih tehnologija (bez obzira da li se radi o EFS-u ili sličnima na drugim platformama). Kao najčešći problem pojavljuje se kriptovanje sadržaja od strane krajnjih korisnika, bez znanja IT-a. Korisnici na taj način smatraju da povećavaju sigurnost podataka, opcija za kriptovanje je im praktično „na dohvat ruke“ u samom korisničkom interfejsu, i kao rezultat imamo neupravljivu strukturu kriptovanja

podataka koja je izuzetno opasna. U takvim se slučajevima certifikati sa ključevima generišu lokalno, a ne centralizovano, vezani su za lokalni korisnički profil i nemaju backup. Postupak poput reinstalacije operativnog sistema ili zamjene računara, bez ranijeg pravilnog eksporta certifikata (što korisnik obično ne uradi jer niti ne zna da je to potrebno) čini da se ključevi trajno izgube a time i pristup fajlovima. Kako enkripcija struktura nije centralizovana (kao u slučaju kada je implementira IT) nema pohrane ključeva na drugo mjesto niti Recovery agenta.

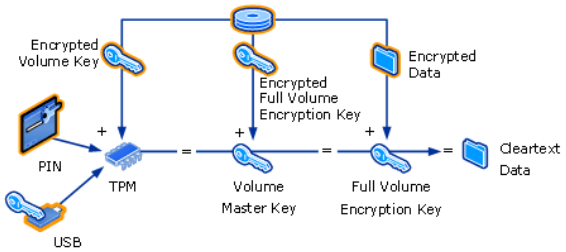
Drugi, takođe dosta tipičan, primjer loše upotrebe je kada IT polovično implementira EFS na nivou domenskog okruženja, bez dovoljno dobrog poznavanja svih komponenti koje učestvuju u tom procesu. Iako se domenskom implementacijom postiže centralizacija, neophodno je posebnu pažnju posvetiti pravilnom backupu i arhiviranju ključeva koje izdaje centralni Certificate Authority. Dok je većina certifikata druge namjene relativno lako zamjenjiva, certifikate za kriptovanje ne možemo zamijeniti – ako izgubimo originalni, a nemamo jasno definisanu proceduru oporavka (kao ni njene potrebne komponente) gubi se i pristup podacima.

Isticanje certifikata za enkripciju, bez podešene automatske obnove, treći je tipičan propust. Svaki certifikat, a time i par ključeva koje on nosi, ima vijek trajanja (obično 12 ili 24 mjeseca). Ukoliko ne dođe do pravilne procedure obnove, prije isticanja ovog vremenskog perioda, certifikat a time i ključevi gube funkciju. Takođe je u ovom slučaju potrebno voditi računa i o tome da se certifikat uvijek obnavlja sa istim parom ključeva.

EFS je i danas u upotrebi, mada dosta manje nego ranije. Njegova efikasnost u smislu sigurnosti nije umanjena, ali je funkcionalnost i mobilnost značajno ograničena, što ga u današnjem vremenu čini dosta nepraktičnim za upotrebu. Ipak, za podatke koji se nalaze u zatvorenim i kontrolisanim okruženjima, ovaj vid enkripcije i danas ima primjenu. Tim prije što je podrška za EFS uključena u sve Windows operativne sisteme te nije potrebno kupovati nikakvu licencu.

III. ZAŠTITA KRIPTOVANJEM DISKOVA (PRIMJER – BITLOCKER)

Kao nešto novija tehnologija koja štiti podatke, Bitlocker, pojavio se prije nekoliko godina kao nešto generalniji način za zaštitu podataka prvenstveno na laptop računarima, koji su najviše podložni krađama. Za razliku od EFS-a, koji vrši zaštitu na nivou fajla (ili direktorijuma) Bitlocker radi na nešto drugačijem principu – umjesto fajlova kriptuje se kompletan disk (ili particija), a u mjesto certifikata i ugrađenih enkripcijskih algoritama koristi se hardverski TPM (Trusted Platform Module) čip koji se nalazi na matičnoj ploči većine prenosnih računara koji su proizvedni u posljednjih 5-6 godina. Primarna namjena Bitlocker tehnologije je da onemogući neovlašteni pristup kompletnom hard disku, budući da se proces otključavanja dešava prije starta operativnog sistema (stoga je za Bitlocker potrebna jedna posebna manja particija na disku) a podacima nije moguće pristupiti ukoliko disk nije u računaru na kojem je originalno postavljena Bitlocker enkripcija, odnosno ukoliko nema komunikacije sa TPM čipom.



Slika 2. Koncept rada Bitlocker-a

Bitlocker tako omogućava da se postigne nekoliko stvari. Prvo, onemogućava se start operativnog sistema dok se ne upiše odgovarajući PIN, kojim se otključava TPM, a iz njega zatim Master ključ koji otključava disk. Time se praktično uvodi još jedan metod verifikacije identiteta korisnika, pored onoga koji svakako postoji na Windows operativnom sistemu. Pored toga, onemogućava se da krađa računara/laptopa ili hard diska, ugrozi sigurnost podataka na njemu. Bez prisustva TPM čipa, odnosno recovery ključa (koji se generiše u momentu aktivacije Bitlockera) nema načina da se pristupi podacima. Bitlocker se može primijeniti i na prenosne diskove, kao i USB stick medije što ga čini dosta široko primjenjivim. Ipak, treba imati u vidu da Bitlocker ne sprovodi nikakvu zaštitu na nivou pojedinačnog fajla (za razliku od EFS-a). Kada korisnik upiše Bitlocker PIN, podigne operativni sistem i logira se na Windows – zaštite više nema. Svi fajlovi koji se pošalju putem maila, postave na cloud storage servise ili na bilo koji drugi način kopiraju ne nose sa sobom nikakvu zaštitu vezano za Bitlocker. Jedna do čestih zabluda vezana za Bitlocker (ili slične tehnologije) je da one daju perzistentnu zaštitu na nivou fajla, poput EFS-a. To nije slučaj, i Bitlocker nije alternativna, nego komplementarna tehnologija EFS-u. Bitno je naglasiti da implementacija Bitlockera može biti upravljiva od strane organizacije, te da se ne bazira na ličnim certifikatima korisnika.

Ipak i pored toga što je pristup implementaciji Bitlocker tehnologije nešto jednostavniji nego kod EFS-a, bitno je naglasiti da i tu može doći do pogrešnih implementacija. Generalno, preporučuje se da i ova tehnologija bude implementirana centralizovano sa kontrolom od strane administratora, umjesto pojedinačno. Slično kao i EFS, korisnik može i samostalno pokrenuti aktiviranje Bitlocker zaštite na svom računaru i time praktično biti odgovoran za pohranu svih kritičnih podataka, od kojih je najznačajniji recovery ključ, koji je neophodan u slučaju regularnog oporavka diska zaštićenog Bitlockerom ili u slučaju gubitka PIN-a, prenosa diska u drugi računar i sl. Centralizacija ovog ključa u domensku AD bazu je mnogo sigurniji pristup nego čuvanje lokalno. Takođe, uvođenje alata za upravljanje Bitlockerom je, po autorovom iskustvu, vrlo preporučljivo, budući da alati koji su dostupni nativno ne daju dovoljno dobar i jasan pregled dešavanju unutar korporativne mreže. Na kraju, veoma je bitno i da se korisnicima dobro objasni šta se postiže sa Bitlocker zaštitom kao i šta se ne postiže. Primjeri iz prakse pokazuju da upravo pogrešno razumijevanje ove tehnologije vodi i pogrešnoj upotrebi a onda i lošoj ili nikakvoj zaštiti.

IV. RIGHTS MANAGEMENT ZAŠTITA (PRIMJER AD/AZURE RIGHTS MANAGEMENT)

Iz dva ranije opisana načina zaštite podataka, koji su najčešće u upotrebi, lako se vide prednosti i mane lokacijski ovisnih metoda zaštite podataka. I EFS i Bitlocker, kao i njima slične tehnologije, su vrlo zavisni od lokacije upotrebe podataka koji su njima zaštićeni. Dok EFS zahtijeva prisustvo certifikata (sa odgovarajućim parom ključeva) da bi se moglo manipulisati zaštićenim podacima, Bitlocker, sa druge strane, zahtijeva prisustvo TPM čipa odnosno recovery ključa, te ne tretira pojedinačne fajlove. To je, u jednu ruku, dodatno osiguranje od neovlaštenog pristupa, no postavimo li ovo u kontekst današnje mobilnosti podataka, načina njihove konzumacije, vrlo varijabilne lokacije kao i velikog broja uređaja, nije teško zaključiti da navedeni metodi odnosno koncepti zaštite ne daju očekivani rezultat. Kako bi se prilagodili današnjem stanju i potrebama kako korisnika, tako i kompanija koje žele zaštititi svoje podatke, neophodno je osigurati zaštitu istih koja ima sljedeće ključne osobine:

- Permanentno je vezana za konkretan fajl bez obzira na lokaciju na kojoj je fajl kreiran odnosno na kojoj se fajl koristi
- Primjenjima je na različitim platformama operativnih sistema
- Ima mogućnost globalne verifikacije identiteta korisnika koji koristi podatake
- Ima mogućnost dijeljenja zaštićenih podataka između ograničenog skupa korisnika
- Ima mogućnost stalnog upravljanja bez potrebe za direktnim kontaktom nad fajlom koji je zaštićen

Ovakvi zahtjevi, za današnje prilike realni, vrlo su visoki sa aspekta tehnologije koja treba da na njih odgovori. Ipak, tehnologija koja može odgovoriti na ove zahtjeve postoji već duže vrijeme i poznata je pod opštim imenom „digital rights management“ (DRM). U masovniju upotrebu, DRM je ušao kroz potrebu za zaštitom multimedijalnih sadržaja na Internet-u. Bilo je potrebno definisati zaštitu koja bi štitila multimedijalne sadržaje (na prvom mjestu muziku i filmove) na način da je se ne može ukloniti u realnom vremenu, da je vezana za identitet korisnika, da definiše upotrebna prava nad konkretnim sadržajem te da je vremenski ograničena (po potrebi). Ovim se postiže da, na primjer, možemo „iznajmiti“ film sa nekog Internet servisa koji ćemo moći gledati samo uz korištenje našeg korisničkog naloga, nećemo ga moći iskopirati, te će njegova upotrebljivost biti ograničena na recimo 24 ili 48 sati (zavisno od onog što smo platili).

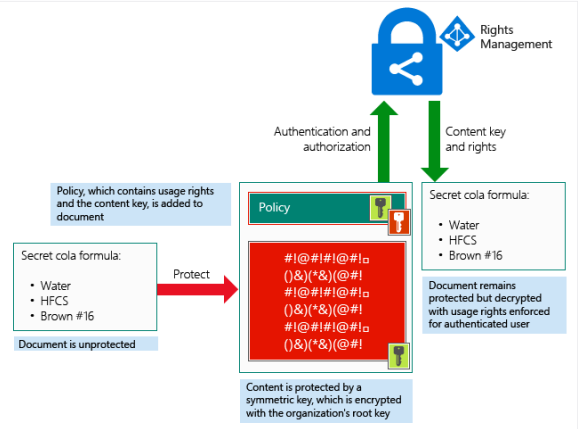
Gotovo paralelno, DRM bazirane tehnologije razvijale su se i za sadržaje koji nisu multimedijalni – prvenstveno za poslovne podatke osjetljivog sadržaja, koji su trebali permanentnu zaštitu koja ne ovisi o lokaciji, niti o platformi koja se koristi za manipulaciju podacima. Danas dominantna tehnologija za ovaj vid zaštite je Active Directory Rights Management odnosno cloud verzija iste pod nazivom Azure Rights Management (koristi se i termin Azure Information Protection).

Ono što je omogućeno unutar pomenute tehnologije je praktično da se adresiraju svi zahtjevi navedeni na početku ovog poglavlja. Rights Management tehnologija takođe se bazira na enkripciji kao osnovnom metodu zaštite, no za razliku od EFS-a, gdje sa enkripcijom zaštita i počinje i završava, rights management koristi još nekoliko dodatnih podataka i parametara. Kao prvo, uvodi se mehanizam provjere identiteta korisnika putem njegovog/njenog korisničkog naloga prilikom svake upotrebe zaštićenog fajla. Naizgled jednostavno, ali zapravo se radi o dosta kompleksnom mehanizmu, jer se podrazumijeva njegova globalna dostupnost. U slučaju implementacije Rights Management tehnologije lokalno, potrebno je servis za autentikaciju objaviti prema Internetu kako bi mogao biti dostupan za provjeru identiteta korisnika i onda kada se zaštićeni fajlovi otvaraju i koriste van kompanije. U slučaju implementacije Rights management tehnologije u cloud-u za korisnika su stvari nešto jednostavnije, jer se bar u slučaju Azure Rights Managementa kao verifikacijski servis koristi Azure Active Directory, koji jeste globalno dostupan. Dalje, uz zaštićeni dokument se definiše i tzv. upotrebna licenca – kao skup prava koja određeni korisnik može ostvariti nad dokumentom. Na primjer, tu se može definisati da li se fajl može printati, kopirati, mijenjati, proslijediti (ako je u pitanju email) i slično. Upotrebnu licencu i taj skup prava (eng. usage rights) definiše autor dokumenta, ručno ili putem predefinisanog predloška. Dodatno, autor može da definiše i trajanje odnosno vrijeme upotrebljivosti tog zaštićenog sadržaja (npr. 7 dana od prvog otvaranja) ali i da u svakom momentu povuče upotrebnu licencu za zaštićeni sadržaj čime isti postaje nedostupan svima koji ga posjeduju, bez obzira u koliko kopija postoji i gdje ga se koristi.

Vrijedi prokomentarisati i način enkripcije koji se ovdje koristi. Za razliku od EFS-a gdje se simetrični ključ štitio ličnim ključem korisnika koji je štitio fajl, pristup kod Rights Management-a je drugačiji. Simetrični ključ se sada kriptuje matičnim ključem organizacije u kojoj je uspostavljen Rights Management sistem, čime se kontrola u značajnoj mjeri sa korisnika prebacuje na korporativni IT. Korisnik u ovom slučaju, tek po verifikaciji identiteta, i provjeri upotrebne license dobija ključ za dekripciju sadržaja. Obzirom da je upotrebna licenca ključni element ove zaštite, dijeljenje ovakve vrste zaštićenih dokumenata zapravo predstavlja definisanje više od jedne upotrebne licence za jednog ili više drugih korisnika. Ponovo, za razliku od EFS-a, ovdje nije neophodna portabilnost korisničkog digitalnog certifikata, odnosno para ključeva, da bi se pristupilo zaštićenim podacima. Obzirom da se većina podataka potrebnih za pristup nalazi u Rights Management sistemu (lokalno ili u cloudu), korisniku je za pristup podacima potrebno samo da ima odgovarajući set kredencijala za verifikaciju svog identiteta, te aplikaciju koja je u stanju da prihvati i primijeni upotrebnu licencu za zaštićeni fajl. Ovaj pristup umnogome olakšava mobilnost zaštićenih podataka, obzirom da je aplikativna podrška, sa klijentske strane, danas dostupna za sve aktuelne platforme, kako mobilne tako i desktop/laptop.

Na kraju, ali ne i najmanje važno, Rights Management tehnologija, u svojoj cloud izvedbi omogućava i praćenje upotrebe zaštićenog sadržaja. Autor sadržaja, odnosno onaj ko je primijenio zaštitu, u mogućnosti je pratiti aktivnosti nad

zaštićenim sadržajem kao i aproksimativnu geo-lokaciju gdje se dokument upotrebljava. Treba reći da se lokacija ne određuje putem GPS servisa, nego korištenjem IP adrese sa koje se pristupa Rights Management servisu što lokaciju ne čini sasvim preciznom.



Slika 3. Koncept rada Rights Management sistema za zaštitu

V. ZAKLJUČAK

Iz navedenog u ovom radu se vidi da je odabir tehnologije za zaštitu podataka slojevit proces u kojem je potrebno uzeti u obzir više faktora. Obično se polazi od pitanja „šta zapravo štitimo?“. Odgovor na ovo pitanje usmjerava nas pri adekvatnom odabiru odgovarajuće tehnologije za zaštitu. U gotovo svim scenarijima, treba uzeti u obzir današnju mobilnost podataka i uređaja, što umnogome utiče i na izbor tehnologije za zaštitu. Ipak, za sve navedene tehnologije važi jedno zajednično pravilo odnosno preporuka – pri njihovoj implementaciji treba svakako težiti ka tome da budu upravljive i po mogućnosti sa centralizovanom kontrolom. Ovakav pristup značajno olakšava implementaciju, održavanje, kontrolu korištenja ali i oporavak zaštićenih fajlova u vanrednim situacijama. Izuzetak od ovoga su primjene tehnologija za zaštitu u privatnim okruženjima, gdje uvođenje dodatnog stepena kontrola najčešće nije potrebno.

LITERATURA

[1] MS Docs: Overview of BitLocker Device Encryption in Windows 10
[2] MS Technet: How EFS Works
[3] MS Docs: What problems does Azure RMS solve?

ABSTRACT

Data protection has always been a current and dynamic topic. However, approach to the data protection, in cases where data location is known in advance, is significantly different from scenarios where data location can not be precisely defined. Consumerization of IT, as a social process that has been going on for several years, has allowed the use of various devices that can process data. We also witness a kind of revolution in IT understanding in general, which is mostly reflected in the omnipresence of cloud technologies. These trends significantly change our approach on data protection. Data, with emphasis on business-like ones, is now present on many different locations and different devices, many of which are unmanaged and uncontrollable by corporate IT. This paper deals with some of the key data protection technologies currently in use, as well as data protection approaches depending on their use scenarios and location. Although the paper refers to some specific technologies in Windows environments, it would be wrong to consider it exclusively oriented to this platform. The Windows operating system is dominant in the laptop / desktop segment, but in the broader sense this is not the case in the field of the device, so we will therefore consider multiplatform technologies wherever possible.

ENCRYPTION TECHNOLOGIES IN MODERN WINDOWS BASED ENVIRONMENTS

Damir Dizdarević