Säker distribution av digital media

Kandidatavhandling av Fredrik Byggmästar 27292

1. Introdkution

Innan Internets storhetstid distribuerades filmer och musik genom fysiska media på CD- och DVD-skivor. Med snabbare Internetanslutningar har distributionsmöjligheterna utvidgats. Sättet som media köps på har också genomgått en förändring. T.ex. tidigare köpte konsumenter hela CD-skivor medan idag är det möjligt att köpa låtar skilda var och en för sig. Idag kan man genom tjänster som Spotify och Netflix också prenumerera på filmer och musik. Att mot en fast månatlig avgift strömma musik och TV-serier direkt från Internet hem till TV-apparaten eller datorn. Apples iTunes erbjuder också motsvarande möjligheter att köpa enskilda låtar istället för hela förvalda samlingar[1]. Även andra typer av underhållning kan köpas direkt över nätet från iTunes. Denna förändring och migrering till Internet har öppnat upp för nya distributionsmöjligheter men också skapat en rad nya problem för företag, leverantörer och mediaproducenter. Många av dem vill nämligen behålla kontrollen över hur media konsumeras. T.ex. tidigare i vintras[2] förbjöd Sanoma Television Oy kunder till Anvias Watson-tjänst att automatiskt spela in eller se på TV-program från deras TV-kanaler: Nelonen, Jim och LIVfrån dator och mobiltelefoner. TV-kanalerna får endast ses genom TV-apparater och STB fastän den bakomliggande IPTV tekniken är identiska för alla klienter. Företagen försöker också åstadkomma lagförändringar som gör det möjligt att jaga personer som bryter mot mediaproducenternas regler. Detta ligger dock utanför ramen för den här uppsatsen. Det görs däremot tekniska lösningar för att påtvinga dessa kontroller. Dessa tekniska lösningar går under namnet Digital Rights Management(DRM) och denna uppsats kommer att se närmare på hur DRM fungerar för att tryggt distributionen media över Internet och hur media konsumtion kan kontrolleras och styras.

2. DRM

DRM är ett samlingsnamn för de tekniker och system som används för att skydda och kontrollera material som distribueras på olika sätt t.ex. över Internet eller på vanliga CD- och DVD-skivor. Teknikerna hjälper till att hålla kontrollen ända från leverantören till konsumenten. Med moderna DRM metoder är det också möjligt att bestämma på vilka sätt konsumenten kan spela upp materialet på. Vilka format materialet görs tillgängligt på.

2.1. Komponenter

Material som distribueras över Internet skickas antingen som filer eller genom strömning.

2.1.1. Filformat

Digital media lagras i filer. Olika filtyper används för olika sorters media. Vanliga filformat är:

- mp3, ogg och wav för ljud
- mpeg för video, filmer och TV-serier
- pdf, doc för böcker och dokument

2.1.2. Enkodning

Innehållet i filerna lagras och komprimeras på olika sätt. Komprimeringen kan antingen kan vara felfri eller destruktiv. Felfri komprimering innebär att all den lagrade informationen går att återskapa exakt när den tolkas medan destruktiv komprimering avsiktligen lämnar bort information. Fördelen med destruktiv komprimering är att datamängden som lagras i filen blir avsevärt mindre till storleken. Nackdelen med destruktiv komprimering är att kvaliteten på innehållet försämras.

2.1.3. Strömning

Strömning av media innebär att media laddas ner dynamiskt i realtid. Detta kan vara t.ex. direktsänd TV eller radio via Internet. Strömning innebär att media filer inte nödvändigtvis lagras hos konsumenten. Istället spelas materialet upp i realtid vartefter det laddas ner. Materialet som strömmas från Internet kan däremot ligga lagrat i filer hos leverantören. Idag används t.ex. [3]MPEG-2 och MPEG-4 som standard för DVB och IPTV sändningar där MPEG Transport Stream(MTS) används som distributions protokoll. MTS är ett fördelaktigt protokoll att använda för strömning eftersom det bl.a. tar i beaktande och kan hantera att datapaket kan försvinna på vägen från avsändaren till mottagaren.

2.2. Tekniker

Det finns en rad intressanta tekniker som används i DRM-systemen. Det här kapitlet ser närmare på dem.

2.2.1. Kryptering

Kryptering innebär att data görs svårare att tolka. Kryptering av data sker med hjälp av krypteringsalgoritmer och krypteringsnycklar. Det finns huvudsakligen två krypteringsmetoder som är intressanta för DRM-system. Dessa två är symmetrisk kryptering och asymmetrisk kryptering. Symmetrisk kryptering innebär att samma krypteringsnyckel används till både kryptering och dekryptering av data medan asymmetrisk kryptering använder två olika krypteringsnycklar, en nyckel för kryptering och en annan nyckel för dekryptering. För att dekryptera ett symmetriskt krypterat meddelande förutsätts att både avsändare och mottagare känner till samma nyckel. Den överlägset mest populära asymmetriska krypteringsalgoritmen i DRM-system är RSA. [4] RSA använder två nycklar, en offentlig nyckel som används för att kryptera

meddelanden med samt en hemlig nyckel som används för att dekryptera meddelanden med.

2.2.1.1. Autentisering

Asymmetrisk kryptering kan användas för att autentisera klienter. Dels för att trygga kommunikationen men också för att garantera att rätt klient får rätt information. Detta förutsätter att varje klient genererar egna RSA-nycklar. Det finns också klienter som levereras med förprogrammerade RSA-nycklar.

2.2.1.2. Algoritmer

Valet av krypteringsalgoritm för innehållet bör väljas efter situation.
Faktorer som påverkar valet:

- direktsändning eller lagring av media
- prestanda på konsumentelektronik

Tyngre algoritmer kräver mera processorkraft. Vid direktsändningar vill man inte ha allt för tung kryptering eftersom direktsändningen dröjer, vid t.ex. sport evenemang. Speciellt om direktsändningen kombineras med andra realtids Internettjänster som Twitter. Man vill heller inte använda en allt för enkel kryptering som är lätt att knäcka.
Dekrypteringsmöjligheter bör också ta i beaktande. Prestanda och pris på konsument elektronik är ibland avgörande. Därför ställs det krav på att dekrypteringen skall kunna ske snabbt även på äldre och långsammare hårdvara. Alla STB-boxar klarar t.ex. inte av att dekryptera sändningar i MPEG-4-kvalitet.

2.2.1.3. Strömning

MPEG Transport Stream(MTS) protokollet innehåller information för krypteringsnycklar. Varje paket innehåller information om paketet är krypterat eller ej. Om paketet är krypterat så anges även vilken krypteringsnyckel som bör användas, udda eller jämn, av de två krypteringsnycklarna. [5]Marlin DRM

krypterar MTS paket med Advanced Encryption Standard(AES) 128-bitars Cliper Block Chaining(CBC). AES är symmetrisk kryptering. Detta betyder att krypterade MTS sändningar bekvämt kan multicastas över UDP.

2.2.2. Licenser

Förutsättningen för att konsumenten ska kunna ta del av DRM-skyddat material hänger på licenser. Licenser bestämmer vilka sätt DRM-skyddat material kan konsumeras på och spelas upp. Licenser innehåller regler för hur dekrypteringen bör ske, vilka krypteringsalgoritmer och nyckel längder som används på materialet samt dekrypteringsnycklar. Metadata om det DRM-skyddade materialet inkluderas också samt möjligheter att koppla ihop licensen med det DRM-skyddade materialet. Licenser kan också innehålla annan väsentlig information, beroende på DRM-system.

2.2.2.1. Licenstyper

Vanligtvis kan giltighetstider specificeras i licenserna. När giltighetstiden går ut förväntas klienten inte längre dekryptera materialet, utan istället vägra att spela upp materialet. Definitionen av giltighetstid öppnar upp för två olika affärsmodeller:

- slutet tidsintervall skapar möjligheten att hyra ut material under en viss tid.
- öppet tidsintervall, d.v.s. tidsintervall som saknar slut tid symboliserar köp av media och oändlig uppspelningstid.

2.2.3. Vattenstämpling

Med hjälp av digital vattenstämpling är det möjligt att bädda in information i media. Denna information kan antingen vara synlig eller osynlig. Den inbäddade informationen följer med när media distribueras och kopieras. På detta sätt är det möjligt att spåra ursprungliga ägare av material och utgivaren av media ifall sådan vattenstämpel har gjorts.

Nackdelar med vattenstämpel är att det eventuellt försämrar kvaliteten på materialet. Vattenstämpling varken förebygger eller försvårar kopiering av data men kan användas för att ta reda på var informationsläckage har skett.

2.3. Ekosystem

Det här kapitlet försöker knyta ihop alltsammans; komponenterna och teknikerna. Hela DRM ekosystemet är ihopkopplat med klienter, infrastruktur och servrar. På serversidan finns en rad funktioner som är relevanta till DRM ekosystem.

2.3.1. Content Delivery System

Content delivery system(CDN) levererar statiskt material. Allt från färdigt krypterade filmer, musik och eböcker och i vissa fall licenser. CDN är en mängd med utspridda servrar runt omkring på Internet som har i uppgift att leverera material, allt från statiska filer till strömmande media. I vissa konfigurationer fungerar CDN som ett mellanlager som avlastar affärslogik servrarna och distribuerar stora datamängder medan i andra situationer kan även CDN hantera affärslogik som t.ex. generering av licenser eller hantera butiksfunktioner. Om DRM-skyddat material är krypterat så kan media spelgas till servrar runt omkring på Internet.

2.3.2. Administrativa verktyg

Till administrativa verktyg hör funktionalitet som används för att styra hela ekosystemet. Dit hör kryptering av nytt material, prissättning, administration av metadata, underhåll av kund databaser osv.

2.3.3. Distribution av licenser

För att distribuera licenser tryggt används kryptering. Olika DRM-system har löst distributionen av licenser på olika sätt. En del utrustar klienterna med färdigt

genererade offentlig och hemlig RSA nycklar vid tillverkningen av klienten medan andra DRM system använder förbättringar av Diffie-Hellman-Merkle nyckel distributions algoritmen. Marlin DRM hämtar licenserna genom Transport Layer Security(TLS).
Ifall tvåvägs datakanal saknas mellan klient och licens server så stöder även några DRM-system distribution av licenser genom USB-minne. Men eftersom datakanalen är begränsad till envägs kommunikation används denna metod oftast vid betal-TV, till skillnad från Video-on-demand.

2.3.4. Klienter

Klienter har som uppgift att spela upp DRM-skyddat material ifall licenser finns tillgängliga och ifall licenserna är giltiga. Eftersom hela kedjan bör vara trygg måste även uppspelning vara säker. Klienterna har i uppgift att ta emot det krypterade materialet, samt avkodningsnycklarna och göra materialet användbart för den betalande slutanvändaren. Förutsättningen för trygghet ligger i att klienten följer reglerna som specificeras i licensen.
Exempel: TV-apparater som stöder Marlin DRM förväntas ha tillgång till Internet. Dessa apparater tar själv kontakt med servrar för att synkronisera tiden. Detta görs för att användaren inte ska kunna ställa om tiden på TV-apparaten manuellt och se på DRM-skyddat material med licenser som har gått ut. Om TV-apparaten saknar Internet eller om TV-apparaten inte lyckas synkronisera tiden mot kända tids servrar så vägrar TV-apparaten att spela upp materialet. Klienterna förutsätter alltså att respektera de regler som licenserna dikterar.

2.4 Angreppsmetoder

Förutsättningen för att DRM ska fungera är att hela kedjan från distributören ända fram till konsumenten är trygg. Detta öppnar upp för en rad

angreppsmetoder. Några av dessa angreppsmetoder ligger utanför ramen för vad DRM kan åstadkomma. Andra angreppsmetoder kan avvärjas. I det här kapitlet kommer vi att gå djupare in på olika angreppsmetoder. Vissa kan begränsas på teknisk nivå medan andra är omöjliga att förhindra.

2.4.1. Baklängeskonstruktion

DRM-skyddet i DVD knäcktes år 1999 genom att baklängeskonstruera mjukvara som användes för att spela upp DVD-skivor och stjäla krypteringsnycklar[6]. Motsvarande baklängeskonstruktion är möjligt att göra med DRM-klient som installeras som program hos konsumenterna, detta gäller både självständiga spelare samt insticksmoduler till webbläsaren. Vissa TV-tillverkare och STB-tillverkare har egna hårdvarukretsar för DRM vilket gör baklängeskonstruktion svårare.

2.4.2 Analogt hål

För att överhuvudtaget kunna ta del av material behöver det omvandlas till ett format som kan förnimmas av människor. Inget DRM-skydd kan förhindra att någon spelar in analoga mediaströmmar som visas på en skärm med extern inspelningsutrustning. Därför ligger denna angreppsmetod utanför DRM-skydd. Nackdelen med att spela in analoga strömmar är att kvaliteten sjunker eftersom detaljer från original sändningen eventuellt uteblir. Denna angreppsmetod fungerar heller inte på interaktiva media som t.ex. datorspel.

2.4.3. Nyckelstöld

Förutsättningen för att spela upp DRM-skyddat material är att dekrypteringsnycklar når klienten. Alla som kommer över dessa nycklar och materialet har möjligheten att dekryptera materialet. Nyckelstöld kan t.ex. ske genom att någon tjuvlyssnar på kommunikationskanalen mellan klient och licensserver. Angriparen kan också antripa kommunikationen genom

man-in-the-middle.

2.4.3.1. Man-in-the-middle

Man-in-the-middle är en sofistikerad angreppsmetod som innebär att all kommunikation mellan avsändare och mottagare går genom angriparen. Vid inledningen tar avsändaren kontakt med mottagaren. Vad avsändaren inte vet är att avsändaren egentligen har tagit kontakt med angriparen, som i sin tur tar kontakt med mottagaren. All kommunikation mellan avsändaren och mottagaren kan därefter avlyssnas och manipuleras av angriparen. Angreppsmetoden utförs mot dåligt designade kommunikations protokoll. T.ex. är Diffie-Hellman nyckel bytes algoritm känslig för man-in-the-middle angrepp. Några slutna DRM-lösningar använder kombinationer av Diffie-Hellamn och RSA att tryggt distribuera nycklar. Andra situationer där man-in-the-middle används är vid dåliga implementeringar.

3. Implementeringar

I det här kapitlet kommer vi att se närmare på hur DRM tekniker tillämpas i olika tjänster och implementeringar.

3.1. Verimatrix

[9]Verimatrix är ett kommersiellt slutet ekosystem där leverantören köper en helhetslösning. Verimatrix tar betalt för hur många klienter som kopplas upp mot systemet. Varje enhet som kopplas upp mot Verimatrix behöver en licens.

3.1.1. Administration

Verimatrix administreras genom SOAP-anrop mot ett API. Där laddas metadata

in om klienter, information om media. Klienter och media kan sättas i grupper. För att en klient eller grupp av klienter ska kunna ta del av media måste klienterna också ges tillstånd till media. Detta görs genom samma API.

3.1.2. Uppspelning

Verimatrix distribuerar insticksmoduler till webbläsare och mobilplattformar som sedan konfigureras och styrs på klientsidan. T.ex. kontrolleras insticksmoduler i webbläsare genom Javascript. Många moderna STB:n som Motorola och DuneHD har inbyggt stöd för Verimatrix.

3.2. HTML5

Det finns inget standardiserat sätt att spela upp DRM-skyddade videon i webbläsare utan insticksmoduler som klarar av nyckelhantering och dekryptering. På initiativ av Netflix, Microsoft och Google försöker standardiseringsorganet W3C fastställa hur DRM kunde integreras direkt in i HTML-sidor[7]. I skrivandets stund är specifikationerna ännu inte klara. W3C har däremot skissat upp följande modell som förslag(Bild 1).

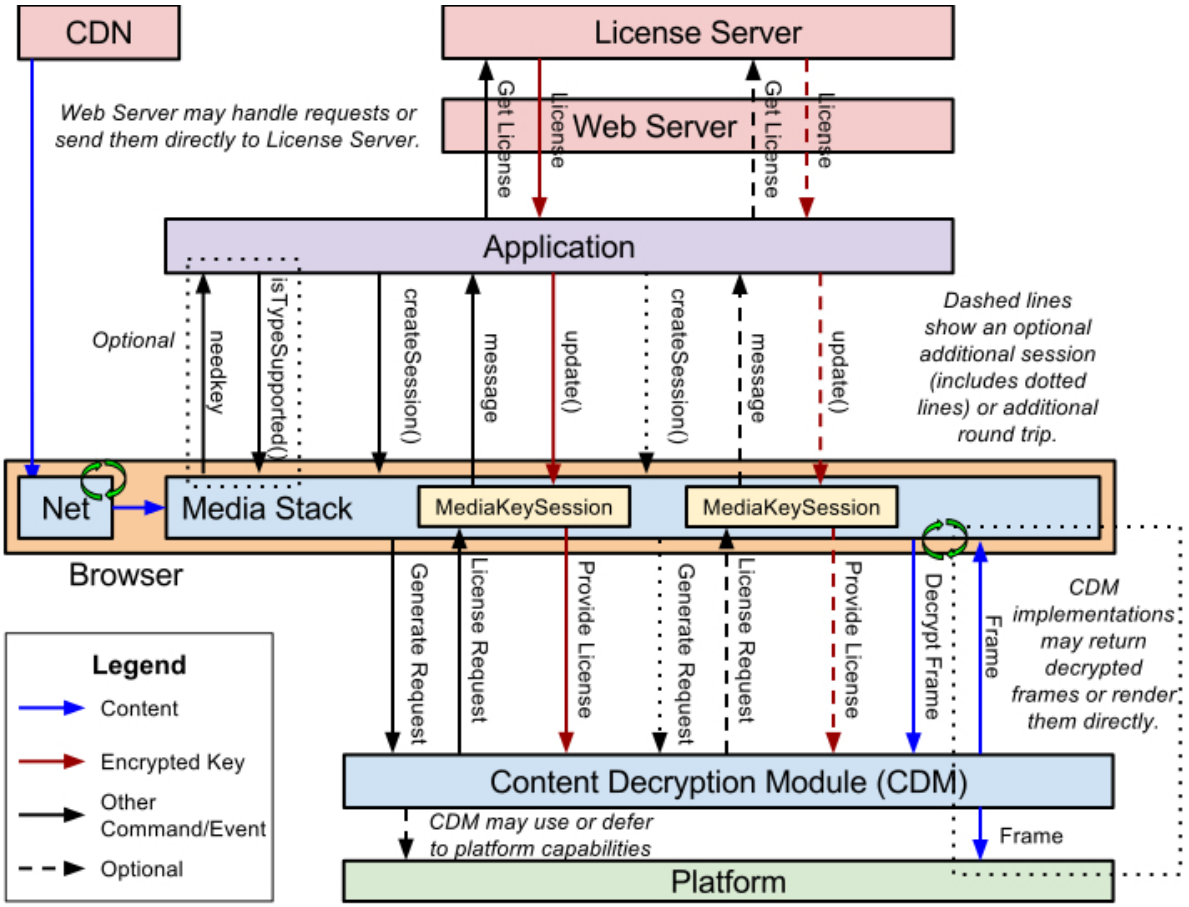

Bild 1, W3Cs förslag på hur HTML5 ska stöda DRM.

3.2.1. Problem

Inbyggt DRM-stöd i HTML löser problemet med insticksmoduler. Problemet är att alla plattformar inte har stöd för alla kodek som eventuellt behövs för uppspelning av media.

3.3. Marlin DRM

[8]Marlin DRM är en DRM teknologi som består av öppna specifikationer gjorda av Marlin Developer Community(MDC). Dit hör specifikationer om hur olika typer av digitalt material levereras till kunden på olika sätt. Allt från strömning av TV-kanaler, filmer och e-böcker. Marlin DRM används bl.a. som nationell IPTV-standard i Japan.

3.3.1. Bakgrund

MDC är ett community som skapar öppna specifikationer till Marlin DRM. Det grundades 2005 av Intertrust, Panasonic, Philips, Samsung och Sony. MDC har som uppgift att föra samman media leverantörer och producenter av konsumentelektronik. Intertrust erbjuder idag ett helt ekosystem baserat på Marlin DRM. Men eftersom specifikationerna är öppna är det möjligt för vem som helst att implementera komponenter eller klienter till systemet. För att få produkter godkända måste de certifieras av MDC.

3.3.2. Action tokens

Action tokens är XML-filer som används för att kommunicera mellan klienter och servrar i Marlin DRM ekosystemet. Licenser specificeras som Action Tokens. Action Tokens i Marlin DRM har också den fördelen att de inte behöver levereras genom nät. Eftersom de är XML-filer kan de bifogas i e-brev eller överföras på USB-minnen.

3.3.3. Verktyg

Marlin levereras med färdiga verktyg som kan köras från kommandoraden. Dessa verktyg kan användas för att kryptera olika typer av media som sedan kan distribueras på Marlin DRM-vänliga ekosystem.

3.3.4. Marlin Simple Secure Streaming Specification

Marlin Simple Secure Streaming Specification(MS3) är den enklaste konfigurationen av Marlin DRM. När materialet skall spelas upp matas licensen in i Marlin klienten. Licensen innehåller nyckel för att kryptera upp materialet.

3.3.5. Överblick

Bild 2 är en överblick över hur MS3 fungerar i praktiken. Användaren bläddrar runt i butiken bland filmer med webbläsare eller annat UI. Efter bekräftat köp kan

klienten ladda ner CAD-filen. En CAD-fil är en XML-fil innehållande information om underliggande krypteringssystem, adressen till krypterat material, undertexter, filstorlek osv, samt adress varifrån licensen kan hämtas. CAD-filen matas in i MS3-klienten med hjälp av Javascript. Det underliggande MS3-systemet tar själv hand om att hämta ner licensen när uppspelningen påbörjar. Från samma CAD-fil får mediaspelaren också adressen till det krypterade materialet.

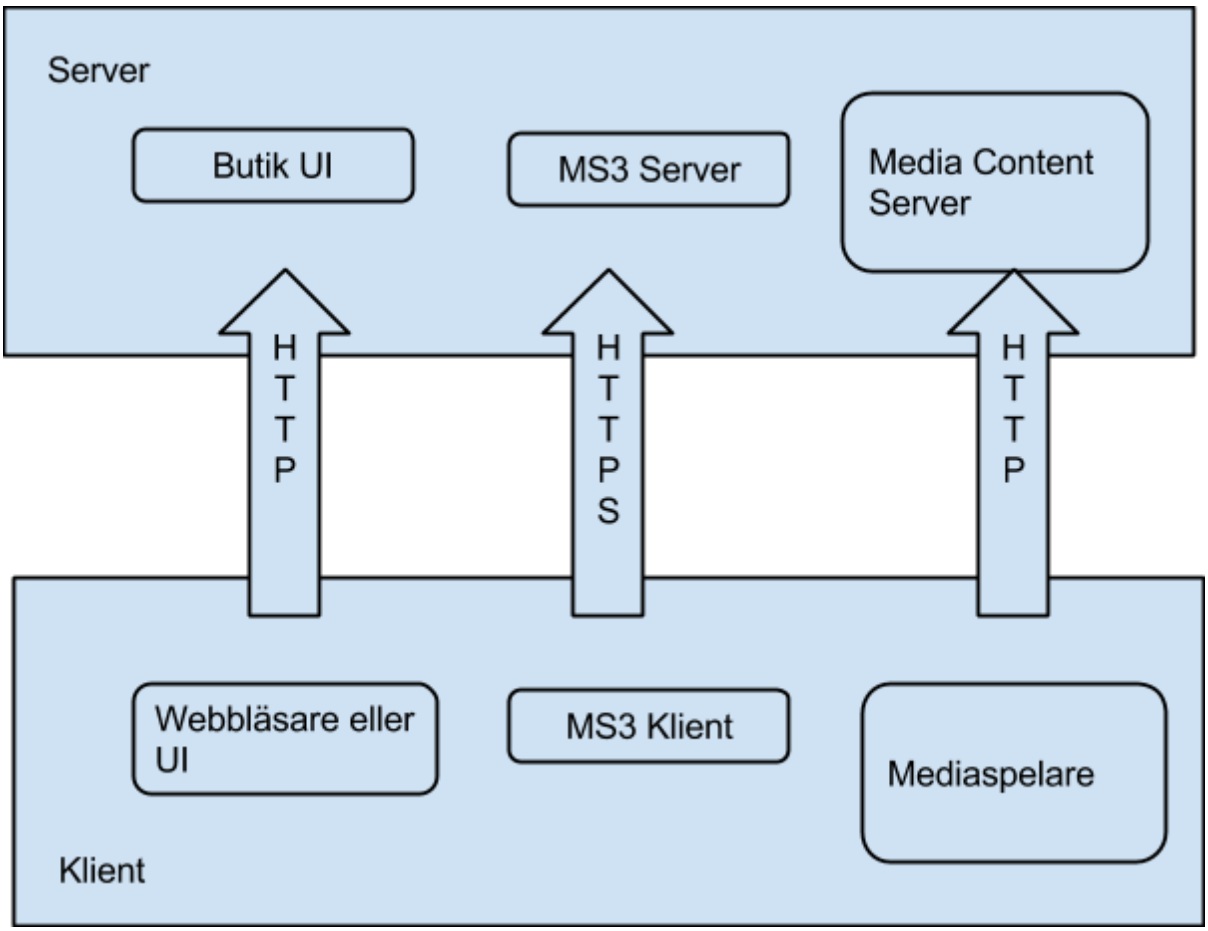

Bild 2, överblick av MS3

3.3.5. Hosted Marlin Service

För att snabbt komma igång med MS3 tillhandahåller Intertrust en molntjänst som genererar Action Tokens som behövs för att driva ett MS3 ekosystem. Priset för genereringen av en Action Token är 0,01€.

4. Kritik mot DRM

[10]Traditionellt är konsumenter vana att äga fysisk media och har möjlighet att spela upp den när och hur de vill. Redan DVD-skivor kunde begränsa vilken landskod en spelare behövde ha för att vara spelbar. Redan detta gav många personer huvudvärk. Ifall semestrande personer köpte DVD-skivor från exotiska länder så var det inte alltid möjligt att dessa var spelbara. Kritiken mot dagens DRM-metoder är värre.

4.1. Säkerhetskopior

Eftersom DRM skyddar mot kopiering så försvårar DRM också tillverkningen av lagliga säkerhetskopior av köpta produkter.

4.2. Batteritid

Enheter många DRM-system förutsätter att klienter är uppkopplade mot Internet innebär det att batteritiden blir lidande eftersom komponenterna som tillhandahåller kontakt till nätet drar ström. Alla DRM-system ger heller inte möljligheten att ladda ner material, vilket förutsätter konstant Internet uppkoppling vid uppspelning. Dessutom är inte Internet alltid tillgängligt.

4.3. Frihet

DRM kan begränsa vilka enheter som har rätt och vilka enheter som inte har rätt att spela upp köpt material. Detta gör att friheten hos konsumenten begränsas.

4.4. Format

Om materialet är låst så begränsar det också möjligheten för kunden att

konvertera formatet till andra format. Detta kan t.ex. ställa till med problem för personer med nedsatt syn och som kräver egen utrustning för att läsa e-böcker.

4.5. Konkurs

Köpt material slutar fungera om leverantören går i konkurs eller om leverantören upphör med tjänsten.

5. Egna reflektioner

Det är ironiskt att företag lägger mycket tid och energi på att försöka förebygga kopiering av material. Speciellt material som finns gratis, olagligt givetvis, i Internets ljusskygga vrår. För att använda analogier om - kedjor och svaga länkar som brister, så lägger DRM ytterligare till en länk i media konsumtionskedjan, vilket försvårar och ökar risken att något kan gå fel för betalande kunder. DRM-system kostar också att implementera och underhålla. Vilket i slutändan innebär högre kostnader för konsumenten, mindre frihet och en mindre tillförlitlig tjänst. Från ett datavetenskapligt perspektiv är det intressant att tillämpa kryptering på olika sätt.

Referenser

[1]http://support.apple.com/kb/ts3599

[2]http://www.tietokone.fi/artikkeli/uutiset/sanoma_kampitti_tv_tallennuspalvelua

[3] ISO 13818 och ISO 14496

[4] A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, R.L. Rivest, A. Shamir, and L. Adleman, 1978

[5] Marlin Broadband Transport Stream Specifications

[6]http://www.cs.cmu.edu/~dst/DeCSS/Kesden/index.html

[7]https://dvcs.w3.org/hg/html-media/raw-file/tip/encrypted-media/encrypted-media.html

[8]http://www.marlin-community.com/

[9]http://www.verimatrix.com/

[10]http://drm.info/