

Hoe DRM de artiest beschermt

Drs. J. Voeten RE en drs. B. de Jonge

DRM heeft de reputatie de consument te beperken in het gebruik van digitale content. De klant downloadt content en betaalt hiervoor, maar wordt gehinderd in het gebruik van de content. Daar staat tegenover dat de rechten van de artiest wel beschermd worden. Is er een mogelijkheid om de rechten van de artiest te beschermen zonder de flexibiliteit in het gebruik van digitale content te schaden? Dit artikel geeft nader inzicht in DRM door de voor- en nadelen te beschrijven. Tevens wordt besproken welke bijdrage de IT-auditor bij het gebruik van DRM kan leveren.

Inleiding

De populariteit van het internet en de steeds sneller wordende verbindingen maken het mogelijk om via een enkele muisklik ringtones, films en andere digitale content binnen te halen ([Mich05]). Het gemak van het downloaden, kopiëren en delen van digitale content heeft reeds geleid tot piraterij. Daarnaast heeft het digitaal aanbieden van media tot gevolg dat het moeilijker wordt om vast te stellen hoe vaak producten zijn verkocht en mogelijk verder zijn gedistribueerd.

Als we praten over online digitale content, waar hebben we het dan eigenlijk over? Voor een definitie van online digitale content verwijzen we naar het artikel 'Bewegingen in de communicatie-industrie' in deze Compact. Zoals in dit artikel tevens is beschreven, zijn diverse partijen betrokken bij de digitale content-waardeketen. Iedere relatie tussen partijen bestaat uit een transactiestroom van aangeboden goederen of diensten enerzijds en een geldstroom anderzijds. Hierbij blijft het altijd de vraag of alle partijen een juiste en volledige vergoeding ontvangen voor de geleverde diensten of producten. Diverse rechtszaken zijn reeds aangespannen door de eigenaren en legale distributeurs om de illegale praktijken te stoppen, maar deze hebben niet het gewenste effect gehad. Verschillende methoden bestaan om zorg te dragen dat de rechthebbende partijen een vergoeding krijgen voor hun diensten en dat de intellectuele eigendommen niet worden geschaad. Eén van deze methoden is Digital Rights Management (DRM).

In dit artikel wordt eerst uitgelegd wat DRM inhoudt. Vervolgens wordt ingegaan op de voordelen van DRM en de bijdrage die DRM kan leveren in de digitale content-waardeketen. Ten slotte wordt besproken wat de rol van de IT-auditor kan zijn in relatie tot het gebruik van DRM.



Drs. J. Voeten RE is adviseur bij KPMG IT Advisory en is specialist op het gebied van informatiebeveiliging, procesanalyse en gegevensanalyse bij zowel publieke als private organisaties. Hij maakt onderdeel uit van het kernteam Communications en Entertainment binnen KPMG IT Advisory en voert veel opdrachten uit binnen de telecombranche. Daarnaast is hij hoofddocent voor de Post-HBO IT Audit-opleiding aan de Haagse Hogeschool.

voeten.jorg@kpmg.nl



Drs. B. de Jonge is als junior EDP-auditor werkzaam bij Ernst & Young EDP Audit. Zijn specialisatie binnen zijn gevolgde opleidingen heeft zich met name gericht op het onderzoeksgebied van Mobile Commerce. Een deel van dit artikel komt voort uit zijn afstudeerscriptie, zijnde de afronding van de studie Information Management aan de Universiteit van Tilburg, waar de toepassing van DRM in een Mobile Commerce-context werd onderzocht. Hij heeft de afstudeeropdracht bij en onder begeleiding van KPMG uitgevoerd.

bas.de.jonge@nl.ey.com

Digital Rights Management

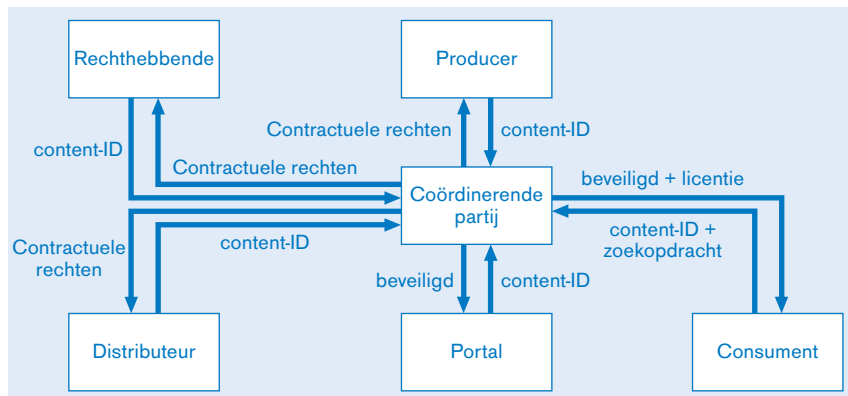
DRM is een populaire term voor een onderzoeksgebied dat zijn intrede deed in het midden van de jaren negentig vanaf het moment dat contentleveranciers, technologieleveranciers en beleidsmakers zijn gaan samenwerken om de distributie van beschermde digitale diensten mogelijk te maken. DRM omvat een aantal activiteiten die uitgevoerd kunnen worden om de rechten op digitale content te definiëren, te managen en te lokaliseren, en maakt hierdoor het beheer van digitale rechten van makers of uitgevers van content makkelijker. De rechthebbenden kunnen, gebruikmakend van DRM, aangeven welke handelingen een gebruiker mag uitvoeren, zonder dat apart toestemming moet worden gegeven ([Wiki07]). DRM kan worden opgesplitst in een drietal deelprocessen:

- *het toekennen van rechten:* het vaststellen van condities voor gebruik, samen met het identificeren van betrokken partijen;
- *het handhaven van rechten:* zorg dragen dat de geïdentificeerde partij de digitale content gebruikt conform de afgesproken condities;
- *het managen van licenties en betalingen:* het uitgeven, beheren en verifiëren van licenties en het zorg dragen voor de betaling behorende bij de licentie ([Jong07]).

Als een partij, verantwoordelijk voor de uitvoering van DRM, aan de waardeketen van digitale content wordt toegevoegd, ziet de waardeketen er mogelijk uit als weergegeven in figuur 1.

Aan de waardeketen is een coördinerende partij toegevoegd die de spil vormt bij het gebruik van DRM om een aantal voordelen te realiseren. De rol van coördinerende partij is in figuur 1 bij een aparte organisatie weergegeven, maar kan ook door één van de eerder onderkende partijen worden ingevuld. De toepassing van DRM in de waardeketen geschiedt meestal niet door de rechthebbende van de content, maar door een coördinerende partij, ook wel intermediair of online distributeur genoemd. In het vervolg van het artikel gaan we ervan uit dat de telecomprovider invulling geeft aan de rol van coördinator. Kenmerkend voor DRM is dat de coördinerende partij in directe relatie

Figuur 1. Digitale content-waardeketen met DRM.



staat met de eindgebruiker. Op het moment dat een gebruiker content downloadt, wordt tegelijkertijd de licentie voor het gebruik gedownload. Deze maakt als het ware deel uit van de gedownloade content. Binnen het DRM-model wordt gebruikgemaakt van technieken om automatisch het overeengekomen gebruik, zoals vastgelegd in de licentievoorzwaarden, te handhaven. Hierbij kan worden gedacht aan encryptie en webservices. DRM is een proces om het gebruik van en de vergoeding voor digitale content te verbeteren. Diverse standaarden zijn hier reeds voor ontwikkeld of worden ontwikkeld, waaronder Secure Digital Music Initiative ([SDMI07]), Microsoft Windows Media Rights Manager (Wind07) en Open Mobile Alliance ([OMA07]).

Voordelen van DRM

Over de toepassing van DRM zijn zowel positieve als negatieve publicaties te vinden. Critici gebruiken vaak de term Digital Restriction Management, waarmee ze hun grootste bezwaar tegen DRM kenbaar maken. Het risico is aanwezig bij een te 'sterk' DRM dat digitale content overmatig wordt beschermd, waardoor het kennismaken van het bestand wordt verhinderd. Daarmee schiet DRM ook aan het beschermen van auteursrechten voorbij, aangezien auteursrechten het doel hebben creativiteit en innovatie te bevorderen. Door te veel beperkingen zullen gebruikers geen kennis nemen van de creatieve uitingen in de vorm van digitale content ([Sche07]).

Nadeel van een te 'zwak' DRM is dat bescherming van digitale content niet wordt gerealiseerd, waardoor de belangen van rechthebbenden niet afdoende worden behartigd. Hierdoor treedt geen noemenswaardige verbetering op ten opzichte van de huidige situatie. DRM zal alleen gebruikt en geaccepteerd worden door alle betrokken partijen als voor hen de voordelen groter zijn dan de nadelen. Dit betekent dat eventuele nadelen die samenhangen met het gebruik van DRM kleiner moeten zijn dan de nadelen in de digitale content-waardeketen zonder het gebruik van DRM of dat de voordelen van DRM opwegen tegen de nadelen van het toepassen van DRM. Laten we eens nader op de voordelen inzoomen.

Directe voordelen van DRM

1. Het beschermen van contractuele rechten: content kan bijbehorende rechten dragen zoals het recht van een auteur (de rechthebbende) op een zelfgeschreven artikel of het recht van een musicus op een opgenomen muziekstuk. Dergelijke rechten zijn vaak erg complex en hebben een bijbehorende financiële regelgeving die afhankelijk is van de mate en soort van gebruik (royalty's). Met behulp van DRM kunnen deze rechten beter worden beschermd.
2. Het volgen van toegang tot of mutaties in de content: informatie met betrekking tot de raadpleging van

content is inherent waardevol voor de leveranciers van content. Door het gebruik van DRM worden deze gegevens bijgehouden en opgeslagen.

3. Het gebruik van licentierechten: leveranciers van content kunnen specifieke licentierechten definiëren om deze beschikbaar te maken met behulp van een contract ([Jong07]). Tevens kunnen via DRM regels aan de consumptie van content worden gesteld, zoals het gebruik in een overeengekomen tijdsperiode of een beperkt aantal keren kunnen afspelen/gebruiken van de content.
4. De consument weet dat digitale content gedownload via DRM legaal is en dat kwaliteit van deze content is gewaarborgd.
5. DRM kan zorg dragen dat de vergoeding die consumenten betalen voor de aangeschafte content, juist en volledig wordt gedistribueerd over de diverse betrokken partijen.

De nadelen die aan het gebruik van DRM kleven komen veelal voort uit individuele acties van fabrikanten waarin beveiliging van content gekoppeld is aan specifieke apparatuur waardoor de content niet flexibel is te gebruiken. Dit wekt frustraties op bij de gebruiker, aangezien een gebruiker die digitale content, zoals muziek, heeft verworven, zelf wil bepalen of hij deze gebruikt op zijn pc, MP3-speler of op beide. Daarnaast wordt verwacht dat DRM een inbreuk kan maken op de privacy van en het gebruikersgemak voor de gebruiker.

Nadelen van een waardeketen zonder gebruik van DRM

1. Diverse partijen zijn betrokken bij de distributie van digitale content, waarbij vaak niet inzichtelijk is wie waarvoor verantwoordelijk is en welke functiescheidingen in de keten aanwezig zijn. Daarnaast is niet voor alle partijen inzichtelijk hoeveel digitale content gedistribueerd is. Dit inzicht wordt deels verschaft door royalty statements, die door andere partijen dan de partij die deze afgeeft, niet of moeilijk op juistheid en volledigheid zijn te controleren. Hierdoor is lastig vast te stellen of alle partijen in de keten de juiste vergoedingen ontvangen voor de geleverde diensten. Ketenpartners wisselen informatie uit en zijn afhankelijk van elkaars informatie over de geleverde diensten. Vertrouwen in elkaars functioneren is een belangrijk punt, maar is niet altijd aanwezig.
2. Momenteel zijn diverse e-commerceprotocollen en webtechnologieën in gebruik bij diverse service providers, waardoor interoperabiliteit in het geding is. Dit leidt ertoe dat er geen of maar beperkt informatie-uitwisseling mogelijk is.

Welke bijdrage kan DRM leveren?

DRM en het beheer daarvan door een intermediair kan meerdere van bovenstaande nadelen uit de digitale

content-waardeketen wegnemen of in ieder geval beperken. Met behulp van DRM kunnen verscheidene verbeteringen worden gerealiseerd.

- Een partij die de coördinatie van het distributieproces van digitale content uitvoert met behulp van DRM draagt ertoe bij dat de verantwoordelijkheden van de ketenpartners verdeeld en helder worden. Deze transparante verdeling van verantwoordelijkheden geeft mogelijkheden tot toezicht en controle op deze verantwoordelijkheden en draagt daardoor bij aan de rechtmatige distributie van mobiele content.

Door de betalingsstromen te controleren draagt DRM bij aan de rechtmatige distributie van mobiele content

- Een betalingskanaal voor het gehele distributieproces, in beheer bij een betrouwbare partij, waarbij alle betrokken partijen de juiste informatie doorspelen naar deze derde partij, leidt tot het vergroten van rechtmatige betalingen. De intermediair legt de gehele procesgang vast en neemt aan de hand hiervan het betalingsverkeer voor zijn rekening. Om dit te bereiken wordt de DRM-beveiliging zo ingericht dat daadwerkelijk duidelijk is waar de content is opgeslagen en/of geraadpleegd bij welke partij. Doordat dit duidelijk wordt, is eveneens helder welke betalingsstromen hierop zouden moeten volgen. Doordat dit te controleren is draagt DRM bij aan de rechtmatige distributie van mobiele content.
- Het DRM-proces stelt dat alle betrokken partijen met elkaar moeten kunnen communiceren. Ten behoeve van de identificatie en verificatie zal er een eenzijdige vorm van communicatie gehanteerd moeten worden. DRM maakt gebruik van standaardprotocollen en een 'message format' ten behoeve van de informatie-uitwisseling. Deze invulling ter verbetering van de interoperabiliteit draagt indirect bij aan de rechtmatige distributie van mobiele content.
- De identificatie van betrokken partijen speelt een belangrijke rol bij het ontwerpen van een betrouwbare DRM-structuur. Het identificeerbaar maken van de eigenaren van mobiele content is op zichzelf niet voldoende. Deze identificatie moet ook naar waarheid verifieerbaar zijn. Wanneer dit het geval is, met behulp van DRM, draagt een beveiligd distributieproces bij aan de rechtmatigheid van de procesgang.

Are you being served?

In de situatie dat er geen gebruik wordt gemaakt van DRM kan de IT-auditor de verschillende partijen in de digitale content-waardeketen op meerdere vlakken van dienst zijn. Uit de huidige ervaringen blijkt dat recht-

hebbende partijen van de content zoals artiesten en producers zekerheid willen hebben dat ze de juiste vergoedingen, royalty's genaamd, ontvangen voor gedownloade digitale content waarvan zij het intellectuele eigendom bezitten.

In het DRM-model kan contractueel het recht van audit worden vastgelegd

Zoals eerder in dit artikel aangegeven staat de coördinerende partij centraal in het DRM-model met als doel alle DRM-gerelateerde processen te managen en de coördinatie en interoperabiliteit te bevorderen. Vanuit het oogpunt van DRM vertrouwen alle betrokken partijen (de rechthebbende, de consument, de distributeur en de DRM-technologieaanbieder) deze coördinerende partij. De coördinerende partij verbindt alle betrokken partijen met elkaar. Logischerwijs wordt deze rol dan ook belegd bij een partij die reeds met meerdere (bij voorkeur alle) partijen in de waardeketen relaties heeft. De rol kan bijvoorbeeld door een telecomprovider worden ingevuld omdat deze al relaties met zowel de consument als de distributeurs en rechthebbende(n) heeft.

Aangezien de intermediair via DRM taken ten behoeve van andere betrokken partijen zal uitvoeren, zullen de afspraken met iedere betrokken partij contractueel moeten worden vastgelegd. Als onderdeel van een der-

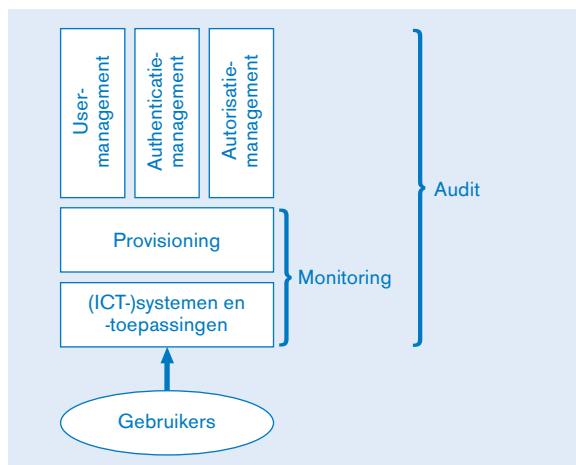
gelijk contract kan het recht van audit of een andere soortgelijke bepaling worden vastgelegd. Hierdoor heeft de 'uitbestedende partij' het recht een audit te laten uitvoeren bij de intermediair, op basis waarvan een bepaalde mate van zekerheid wordt verkregen ten aanzien van de juistheid, tijdigheid en volledigheid van de activiteiten zoals die door de intermediair worden uitgevoerd. Als de betrokken partijen zekerheid willen verkrijgen zijn er vanuit de governancegedachte meerdere mogelijkheden aanwezig om deze te verkrijgen.

De meest gebruikelijke mogelijkheden zijn een Third Party Mededeling (TPM) of een specifieke vorm daarvan, een SAS 70-verklaring. Afhankelijk van de initiatiefnemer kan gekozen worden voor één van deze opties. Een (generieke) SAS 70-verklaring geeft een onafhankelijk en onpartijdig oordeel over het realiseren van 'control objectives', zoals deze door de auditee zijn gekozen. Op basis van een SAS 70-verklaring, en dan bij voorkeur een type 2-verklaring die inzicht geeft in de werking van beheersingsmaatregelen gedurende een tijdsperiode, kan de intermediair aantonen dat hij de DRM-processen dusdanig heeft ingericht dat het intellectuele eigendom van de partijen wordt bewaakt en alle partijen de vergoeding krijgen waar ze contractueel recht op hebben. Dit type generieke verklaring geeft geen beeld ten aanzien van specifieke vereisten van de individuele partijen. Het is een generieke verklaring ten behoeve van de huidige en mogelijk toekomstige betrokken partijen. Als een specifieke partij wil weten of aan haar vereisten is voldaan, of anders gezegd dat de beheersingsmaatregelen zijn getroffen en adequaat werken om aan haar vereisten te voldoen, is een TPM of specifieke SAS 70 een geschikt middel. Deze verklaringen geven een oordeel over beheersingsmaatregelen met betrekking tot specifiek verzochte onderwerpen.

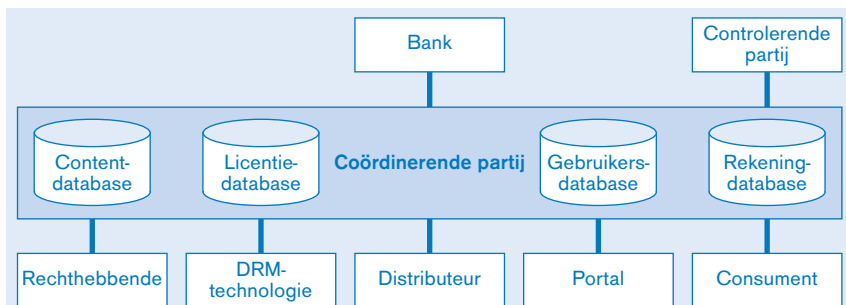
Door middel van een audit, met als resultaat een TPM of SAS 70-verklaring, wordt beoordeeld of de intermediair in de DRM-processen voldoende beheersingsmaatregelen heeft getroffen om gedefinieerde control objectives te realiseren. Dit is grafisch weergegeven in figuur 2. De gebruikers zijn in de figuur de betrokken partijen, waarbij de overige vlakken de activiteiten van de coördinerende partij voorstellen. De intermediair monitort zelf of de provisioning (het uitleveren van content) juist en volledig wordt uitgevoerd. Voor het leveren van de diensten, alsook de registratie van de diensten worden ICT-toepassingen zoals internetportals en databases gebruikt. Daarnaast zijn de DRM-processen ingericht, met daarin de maatregelen om de rechten toe te kennen en te beheren en licenties te verlenen, en zorg te dragen voor betalingen behorend bij de afgegeven licenties.

In figuur 3 wordt weergegeven dat alle betrokken partijen individueel gekoppeld zijn aan de coördinerende partij. Dat wil zeggen dat iedere vorm van gegevens-

Figuur 2. DRM-scope voor TPM- of SAS 70-verklaring.



Figuur 3. DRM-informatie.



overdracht met betrekking tot digitale content tussen betrokken partijen via deze coördinerende partij zal verlopen. De intermediair maakt gebruik van DRM om de belangen van alle partijen te behartigen.

Om de belangen te behartigen heeft de intermediair verschillende databases, namelijk een contentdatabase, een licentiedatabase, een gebruikersdatabase en een rekeningdatabase. Deze databases bevatten noodzakelijke informatie voor de verschillende processen, zoals de transactie, de betaling en DRM. De contentdatabase bevat alle downloadbare content die door betrokken leveranciers is verstrekt. Als een consument of mobiele gebruiker een aanvraag doet voor een bestand wordt de betreffende content opgezocht in de database en bezorgd bij de gebruiker. In de licentiedatabase zijn de licentiedocumenten voor alle mobiele gebruikers opgeslagen. Ieder licentiedocument geeft de eigenaren van de content weer (rechthebbende(n), consument, etc.) samen met de transactiedatum en kosten. De gebruikersdatabase is een database met alle geregistreeerde gebruikers met de bijbehorende persoonlijke informatie en betalingsinformatie.

De coördinerende partij heeft een beveiligde verbinding met een bank en zal op grond van de informatie uit het DRM-proces de betrokken partijen rechtmatig betalen. Doordat de coördinerende partij wordt voorgesteld als mobiele operator zal deze zorg dragen dat de gedistribueerde content in rekening wordt gebracht op basis van bestaande regelingen in de mobiele telefonie in een postpaid situatie. Bij een prepaid consument controleert de operator of de betreffende vergoeding kan worden afgeboekt voordat de content wordt toegekend. Betalingen kunnen ook op een andere wijze worden uitgevoerd, denk hierbij aan IDEAL, waarmee direct een betalingsopdracht wordt gegeven, of aan betalingen via creditcard.

De auditor geeft de betrokken partijen inzicht in de beheersingsmaatregelen die de coördinerende partij heeft getroffen om het betalingsproces op integere wijze uit te voeren. Deze partij heeft namelijk de verantwoordelijkheid voor het gehele betalingsverkeer. Met deze verantwoordelijkheid zijn kosten gemoeid om de uitvoering ook volgens afspraak te verwezenlijken. Deze proceskosten zullen worden doorberekend naar de betrokken partijen. Dit is bijvoorbeeld mogelijk door de proceskosten door te berekenen als fee in de prijsstelling. De centrale gedachte achter deze aanpak is het centraliseren van het betalingsproces bij de coördinerende partij en de leveranciers van content, en vertrouwelijke informatie van de consument te verlangen tijdens de transactie en betaling. De betrokken content providers ontvangen de betalingen van de coördinerende partij en deze partij zal de consumenten de bedragen in rekening brengen. Het grote voordeel van deze methode van betaling is dat consumenten niet langer vertrouwelijke persoonlijke informatie hoeven

te verschaffen bij een onbetrouwbare handelaar, hetgeen de privacyaspecten ten goede komt. Hiervoor wordt een betrouwbare beveiligde verbinding gerealiseerd met de telecomprovider waar de consument al een relatie mee heeft. De auditor kan een bijdrage leveren door bovenstaand betalingsproces ten behoeve van betrokken partijen te auditen.

De coördinerende partij is verantwoordelijk voor een integere uitvoering van het betalingsproces

Conclusie

DRM kan voor meerdere partijen een nuttige bijdrage leveren, maar zal alleen als oplossing voor het schenden van het intellectueel eigendom en het mislopen van vergoedingen worden geaccepteerd als rekening wordt gehouden met technologische, economische, wettelijke en maatschappelijke zorgen. Vanuit een technologisch aspect zal zorg moeten worden gedragen dat de functionaliteit van DRM gebruikersvriendelijk is. In economisch opzicht betekent dit dat gebruikers de digitale content in diverse formaten en via diverse diensten tot hun beschikking moeten kunnen krijgen. Het aanbieden van digitale content in diverse formaten en diensten kan leiden tot nieuwe businessmodellen en het tot stand komen van nieuwe waardeketens. Wetgeving met betrekking tot intellectueel eigendom zal internationaal moeten harmoniseren daar het aanbieden van digitale content niet gebonden is aan nationale grenzen. Tot slot, en dit is waarschijnlijk de grootste uitdaging: het is essentieel consumenten ervan te overtuigen dat DRM geen belemmering vormt, maar het mogelijk maakt legaal te genieten van digitale content en daarnaast toegevoegde waarde levert.

De IT-auditor kan een bijdrage leveren aan de acceptatie van DRM. De auditor kan het vertrouwen in DRM vergroten door zekerheid te bieden aan belanghebbenden dat DRM zorgt voor het beschermen van intellectuele eigendomsrechten en de financiële vergoeding daarvoor. Anders gezegd: de auditor geeft zekerheid dat de partij die DRM beheert ten behoeve van andere stakeholders in de digitale content-waardeketen, afdoende maatregelen heeft getroffen om de juiste werking van DRM te waarborgen. Dit is mogelijk door voor belanghebbenden een specifieke Third Party Mededeling af te geven waarin aangegeven wordt dat de gemaakte afspraken worden nageleefd. Een andere mogelijkheid is een generieke verklaring waarin wordt aangegeven dat DRM dusdanig is ingericht dat de belangen van andere partijen binnen de keten worden gewaarborgd.

Literatuur

- [Jong07] B. de Jonge, *Een onderzoek naar de toepassing van DRM ter bewaking van het distributieproces van mobile content*, 2005.
- [Mich05] S. Michiels, W. Joossen, E. Truyen en K. Verslyppe, *Digital rights management: a survey of existing technologies*, november 2005.
- [OMA07] *Open Mobile Alliance*. <http://www.openmobilealliance.org>. Geraadpleegd 2007.
- [Sche07] *Het auteursrecht in de informatiemaatschappij*, <http://www.ecp.nl/nieuws>. Geraadpleegd juli 2007.
- [SDMI07] *SDMI Home*. <http://www.sdmi.org>. Geraadpleegd 2007.
- [Wiki07] *Wikipedia*. <http://nl.wikipedia.org>. Geraadpleegd 2007.
- [Wind07] *Windows media*. <http://www.microsoft.com/windows/windowsmedia/default.aspx>. Geraadpleegd 2007.