Universidade Federal de Santa Catarina
Curso de Pós-Graduação em Ciência da Computação

Jean Pierre Ezequiel

Estrutura de uma Arquitetura para Digital Rights Management: Um Plug-in para Controle do Uso de Conteúdos Digitais

Dissertação submetida à Universidade Federal de Santa Catarina como parte dos requisitos para a obtenção do grau de Mestre em Ciência da Computação.

Prof. Dra. Carla Merkle Westphall
Orientadora

Florianópolis, dezembro de 2003.

Estrutura de uma Arquitetura para Digital Rights Management: Um Plug-in para Controle do Uso de Conteúdos Digitais

Jean Pierre Ezequiel

Esta Dissertação foi julgada adequada para a obtenção do título de Mestre em Ciência da Computação especialidade em Sistemas de Computação, e aprovada em sua forma final pelo Programa de Pós-Graduação em Ciência da Computação.

Prof. Dr. Fernando A. Ostuni Gauthier
Coordenador do Programa de Pós-Graduação em Ciência da Computação

Banca Examinadora

Prof. Dra. Carla Merkle Westphall
(orientadora)

Prof. Dr. Joni da Silva Fraga
Professor externo ao CPGG residente em Santa Catarina

Prof. Dr. Alexandre Moraes Ramos
Professor do CPGCC

Prof. Dr. Arthur Ronald de V. Buchsbaum
Professor do CPGCC

Florianópolis, dezembro de 2003.

"Oh!Que saudades que tenho
Da aurora da minha vida,.
Da minha infância querida
Que os anos não trazem mais!
Que amor, que sonhos, que flores,
Naquelas tardes fagueiras,
Á sombra das bananeiras,
Debaixo dos Laranjais!
Livre filho das montanhas,
Eu ia bem satisfeito,
-Pés descalços, braços nus-
Correndo pelas campinas
À roda das cachoeiras,
Atrás das asas ligeiras
Das borboletas azuis!"

(Casimiro de Abreu – Meus Oito Anos)

DEDICATÓRIA

Dedico primeiramente a Deus, pois sem Ele nada poderia ser realizado. Aos meus irmãos George e Geison, aos meus amados pais Zenon Antunes Ezequiel e Márcia Aparecida Ezequiel, que tanto me incentivaram e me apoiaram para alcançar este mérito. A todos os amigos e pais espirituais.

AGRADECIMENTOS

É com grande estima que agradeço a todas as pessoas que auxiliaram direta ou indiretamente no desenvolvimento deste trabalho.

Agradeço aos meus amados pais Zenon Antunes Ezequiel e Márcia Aparecida Ezequiel pela vida, pelo constante apoio e incentivo, e pela educação que me deram. Aos meus queridos irmãos, cunhadas, familiares e amigos, que tanto incentivaram e apoiaram-me por todo o caminho que percorri e ainda vou percorrer.

Agradeço a minha namorada Claúdia, que soube conviver com os vários momentos de dificuldade, e que entendeu as diversas vezes em que não pude estar junto.

Agradeço também a Professora Carla Merkle Westphall, que me orientou neste trabalho sem medir esforços e soube conduzir sempre da melhor maneira possível, apoiando e acreditando em mim, mesmo quando dizia “agora sim, eu estou nervoso ou tudo isso!”.

Agradeço ao Professor Carlos Becker Westphall, que sempre ajudou de forma direta ou indireta na vida acadêmica e até mesmo na vida pessoal, quando não parava de falar suas experiências de vida em outros países.

Aos professores Joni da Silva Fraga, Alexandre Moraes Ramos e Arthur Ronald de V. Buchsbaum, que aceitaram com enorme entusiasmo participarem da banca examinadora e que são peças essências para o desenvolvimento de trabalhos futuros.

À UFSC também vai o meu agradecimento pelo suporte de material, infra-estrutura e professores.

Aos professores que estiveram dispostos a ajudar e repassar suas experiências.

Segue também o agradecimento ao professor Alexandre Moraes, o qual freqüentei uma de suas disciplinas e que foi de extrema valia para meu desenvolvimento profissional e deste trabalho.

Agradeço aos amigos Cleber, Felipe, Marcos, Michel, Wesley, Gláucio, Twu, Parra, Marcelo, Alexandre, Rafael, Silvia, que souberam me auxiliar nos estudos e também foram especiais sempre que precisei. Levarei amizade de cada um eternamente no meu coração, Obrigado por serem assim!

Aos amigos da UNIPLAC e UFMG, professores Marcos Piching, Alexandre Perin e Rodrigo Pagliares.

A Verinha (CPGCC), pelo apoio e excelente atendimento aos mestrandos (aplausos para você!).

Por fim, agradeço ao Criador Maior nosso Deus, grande amigo! Te devo mais uma!

SUMÁRIO

LISTA DE ABREVIATURAS

API	*Application Programing Interface*
ASP	*Active Server Pages*
B2B	*Business to Business*
B2C	*Business to Consumer*
C2C	*Consumer to Consumer*
CS	*Control set*
DDL	*Data Definition Language*
DES	*Data Encryption Standard*
DOI	*Digital Object Identifier*
DML	*Data Manipulation Language*
DRPL	*Digital Rights Property Language*
EMMS	*Electronic Media Management System*
ER	*external repository*
HTML	*Hypertext Markup Language*
HTTP	*Hypertext Transfer Protocol*
IAA-QM	*Identification, Authentication Authorization -Query Module*
IBM	*Business International Machines*
IDEA	*International Data Encryption Algorithm*
IDF	*International DOI Foundation*
IP	*Internet Protocol*
IPSEC	*Internet Protocol Security*
ISBN	*International Standard Book Numbers*
JCE	*Java Cryptography Extension*
JCA	*Java Cryptography Architecture*
JSSE	*Java Secure Socket Extension*
JVM	*Java Virtual Machine*
MP	*Message push*
MPEG	*Motion Pictures Experts Group*
OASIS	*Organization for the Advancement of Structured Information Standards*

ODBC	Open Data Base Connectivity
ODRL	*Open Digital Rights Language*
P2P	*Peer-to-Peer*
PBT	*Payment-Based Type*
PFT	*Payment-Free Type*
PHP	*Personal Home Page*
RAS	*Remote Access Server*
REL	*Rights Expression Language*
RG	*Registry Geral*
RSA	*Rivest Shamiry Adleman*
SABDRM	*Security Attribute Based Digital Rights Management*
SDK	*Software Development Kit*
SSL	*Secure Socket Layer*
SQL	*Structure Query Language*
TCP/IP	*Transmission Control Protocol / Internet Protocol*
TI	*Tecnologia de Informação*
UCON	*Usage Control*
URL	*Uniform Resource Locator*
VM	*Virtual machine*
XML	*Extensible Markup Language*
XrML	*Extensible Rights Markup Language*

LISTA DE FIGURAS

LISTA DE TABELAS

RESUMO

Em um mundo onde o comércio eletrônico pela Internet cresce todos os dias, é cada vez maior a procura por soluções seguras e confiáveis para a distribuição de conteúdos digitais. Na busca pela segurança digital, usuários acreditam no estabelecimento de novas tecnologias que possam garantir seus direitos e preservar a propriedade intelectual dos autores e seus conteúdos. O gerenciamento dos direitos digitais vem despertando o interesse da comunidade científica, através de publicações e propostas que objetivam solucionar o uso desautorizado de conteúdos e preservar a integridade da informação digital.

Sendo assim, este trabalho tem como uma de suas finalidades apresentar uma proposta de arquitetura para DRM - *Digital Rights Management,* bem como o desenvolvimento de *software plug-in* para o gerenciamento do conteúdo e dos direitos no lado do cliente. A Arquitetura é composta por vários elementos que juntos podem oferecer maior segurança na distribuição de conteúdos digitais. O *plug-in*, cifra o conteúdo e o armazena juntamente com os direitos no computador cliente. *O plug-in* é responsável também pela decifragem e leitura dos direitos, processo que ocorre somente no momento em que o usuário solicitar a abertura do conteúdo digital. Visando o desenvolvimento da tecnologia o trabalho demonstra pesquisas e resultados importantes para evolução do *Digital Rights Managemen*t.

ABSTRACT

In a world where the electronic commerce by the Internet grows every day, the search for secure and reliable solutions for the distribution of digital contents is the more each time. In the search for digital security, the users believe in the establishment of new technologies that can guarantee its rights and preserve the authors' copyright and contents. The digital rights management is gaining the interest of the scientific community, through publications and proposals that target to solve the problem of unauthorized use of digital contents and to preserve the integrity of the digital information.

Thus, this work has as one of its purposes to present a proposal of architecture for DRM - Digital Rights Management, as well as the development of a plug-in for the management of the content and the rights in the customer side. The architecture is composed for some elements that together can offer greater security on the distribution of digital contents. The plug-in, ciphers the content and stores it along to the rights on the customer's computer. The plug-in is also responsible for the decryption and reading of rights, this process only occurs at the moment that the user requests the opening of the digital content. Aiming the development of the technology the work demonstrates researches and important results for evolution of the Digital Rights Management.

1 Introdução

O crescimento considerável de informações que circulam pela rede mundial de computadores gera uma ampliação no comércio digital, motivando por conseqüência o aumento de falsificações de produtos digitais. Por este motivo é cada vez maior a busca por modelos de "comércio digital de sucesso", os quais requerem arquivos digitais que sejam facilmente distribuídos para múltiplos usuários, preocupando-se em manter os direitos de acesso em ambiente controlado.

Na procura do preenchimento desta lacuna e para assegurar a propriedade intelectual, o DRM (*Digital Rights Management*) vem tornando-se a tecnologia para gerenciar a segurança, o acesso, o uso e reprodução de arquivos digitais, seja *on-line* ou *off-line*, visando garantir que somente pessoas com acesso autorizado possam usar os produtos digitais. De acordo com estudos realizados [59], DRM é o processo de gravação, transmissão, interpretação, garantindo os direitos autorais e que tem como objetivo impedir o uso desautorizado e preservar a integridade da informação digital. Neste sentido existe a necessidade de se padronizar a maneira como ocorre a comunicação dos direitos com os sistemas que são capazes de garantir os direitos definidos.

Sendo assim, este trabalho está trabalho está inserido nesse contexto de pesquisa de *Digital Rights Management.*

1.2 Objetivos do trabalho

O objetivo geral deste trabalho é propor elementos que compõem uma arquitetura para *Digital Rights Management*, e desenvolver um protótipo de um *plug-in* capaz de gerenciar o conteúdo e os direitos no lado do cliente.

A estrutura que engloba os elementos e o *plug-in* deverá ser capaz de disponibilizar um determinado conteúdo e um serviço na *web,* para que possa ser efetuado o *download* do mesmo, garantindo uma licença para sua utilização.

Para atingir estas metas, são definidos os seguintes objetivos específicos:

a) Levantamento e análise das necessidades de segurança do gerenciamento de direitos digitais;
b) Composição de uma arquitetura DRM para controlar o uso de conteúdos digitais;
c) Resolver problemas relacionados com o *plug-in* no lado do cliente;
d) Implementação dos elementos da arquitetura proposta, através de protótipos;

1.3 Justificativas

A tecnologia www oferece o acesso remoto a informações independente de equipamentos e localização, desde que os equipamentos estejam instalados e configurados de forma adequada, de modo a permitir o acesso à rede. Por este motivo a segurança na transmissão de conteúdos digitais é um fator primordial nas transações.

Algumas justificativas que podem ser citadas para o desenvolvimento deste trabalho são as seguintes:

a) Dificuldade em localizar aplicações que forneçam opções seguras para a distribuição do conteúdo;
b) A falta de pesquisas e estudos realizados na área, e que possam contribuir para o crescimento da tecnologia DRM *digital rights management;*
c) O amplo comércio editorial que busca soluções para proibir ou ao menos dificultar a quebra do *copyright;*

d) A carência de arquiteturas e formas que demonstrem como e onde os direitos devem ser armazenados.

1.4 Delimitação do Escopo do Trabalho

Este trabalho propõe uma arquitetura para um sistema DRM. O termo arquitetura denota neste trabalho as partes que interagem no sistema DRM e as mensagens trocadas entre as partes do sistema *digital rights management.*

Além da proposta da arquitetura, este trabalho limita-se especificamente a resolver alguns problemas relacionados com o plug-in no lado do cliente, controlando o uso de documentos em formato simplificado, para efeitos de teste.

1.5 Organização do texto

Para melhor compreensão da proposta apresentada neste trabalho, o mesmo é dividido em oito capítulos. O capítulo introdutório, procura descrever a motivação e os objetivos do trabalho. O capítulo dois é responsável por proporcionar uma introdução à segurança, através da demonstração de conceitos, mecanismos e fundamentos. Já o capítulo três apresenta alguns meios de distribuição de documentos e seus respectivos exemplos.

Digital Rights Management, conteúdo e direitos digitais, bem como tecnologias existentes na área, são apresentados no capítulo quatro. Quanto ao capítulo cinco, alguns trabalhos correlatos são focalizados. O capítulo seis relata ferramentas para implementação. A proposta de arquitetura, assim como o protótipo do *plug-in* desenvolvido são encontradas no capítulo sete. O capítulo oito apresenta as conclusões, incluindo perspectivas e principais contribuições.

2 Conceitos Básicos de Segurança

A informação é considerada um dos principais patrimônios de uma organização, e que está também sob constante risco [6].

Na época em que as informações eram armazenadas somente em papel, a segurança era relativamente simples; Com as mudanças tecnológicas e o uso de "grandes computadores" *mainframes*, a estrutura de segurança ficou mais sofisticada. Com a chegada dos computadores pessoais e das redes de computadores, os aspectos de segurança atingiram tamanha complexidade, que há a necessidade do desenvolvimento de equipes cada vez mais especializadas para sua implementação e gerenciamento. As informações contidas em sistemas computacionais são consideradas recursos críticos, tanto para concretização de negócios como na tomada de decisões [2], e como sistemas de informação institucionais estão conectado em redes externa, maior é a facilidade para a ocorrência de ataques. Outro aspecto a ser considerado pela gerência é que os sistemas de informática, para operarem de forma adequada e garantirem a segurança das informações da organização, necessitam de ambientes controlados, protegidos até contra desastres naturais (incêndio, terremoto, enchente), falhas estruturais (interrupção no fornecimento de energia elétrica, sobrecargas elétricas), fraudes e outros.

Segundo [10], segurança é uma forma de prevenir ações não autorizadas de usuários de sistemas de computadores. Segurança é, portanto, a proteção de informações, sistemas, recursos e serviços contra desastres, erros e manipulações sem licenças, de forma a reduzir a probabilidade e o impacto de incidentes de segurança [2].

2.1 Propriedades da Segurança

Um sistema computacional é considerado seguro se houver uma garantia de que é capaz de atuar exatamente como esperado, satisfazendo as seguintes propriedades que devem ser mantidas no sistema [7]:

- ✓ Confidencialidade – as informações devem ser protegidas contra acesso de qualquer pessoa não autorizada. Esta propriedade envolve medidas como controle de acesso e criptografia.

- ✓ Privacidade – as informações devem ser trocadas mantendo privacidade (quando necessário), sem que possa ser visualizada por outros, ou seja, indevidamente.
- ✓ Integridade dos dados – evitar que dados sejam apagados, ou alterados sem a permissão devida.
- ✓ Disponibilidade – garantir o funcionamento do serviço de informática, sob demanda, sempre que necessário aos usuários autorizados. As medidas relacionadas a esse objetivo podem ser duplicação de equipamentos/sistemas e *backup*. Um bom exemplo de ataque contra disponibilidade é a sobrecarga provocada por usuários ao enviar enormes quantidades de solicitação de conexão com o intuito de provocar indisponibilidade nos sistemas.
- ✓ Consistência – certificar-se de que o sistema atua de acordo com a expectativa dos usuários.

Deve-se estabelecer algumas questões que são de extrema importância para se manter essas propriedades:

- ✓ O que se proteger?
- ✓ Contra que ou quem?
- ✓ Quais as ameaças mais prováveis?
- ✓ Qual a importância de cada recurso?
- ✓ Qual o grau de proteção desejado?
- ✓ Quanto tempo, recursos humanos e financeiros se pretende gastar para atingir os objetivos de segurança desejados?
- ✓ Quais as expectativas dos usuários e clientes em relação à segurança de informações?
- ✓ Quais as conseqüências para a instituição se seus sistemas e informações forem corrompidos ou roubados?

Após o esclarecimento destas questões, procura-se definir uma política de segurança e estudo das ameaças, gerando assim uma análise prévia dos riscos que pode-se enfrentar. Lembrando que a tecnologia de segurança a ser implantada deve estar de acordo com a política. Por fim, para administrar os sistemas, se faz necessário implantar uma gerência de segurança [3].

2.2 A Política de Segurança

A política de segurança de um sistema é um conjunto de regras e práticas que determinam a maneira pela qual as informações e recursos são gestionados, protegidos e distribuídos no interior de um sistema específico [60].

Em busca da integração às metas de negócio da organização e ao plano de informática, a política de segurança acaba gerando impacto em todos os projetos, tendo como exemplos, planos de contingências[1] ou até mesmo planos de desenvolvimento de novos sistemas, onde neste caso a ligação entre política e plano é de extrema importância. É indispensável lembrar que a política não envolve apenas a área de informática, mas todas as informações da organização.

A figura 1, procura mostrar como ocorre o envolvimento entre a estratégia geral da organização com a política de segurança.

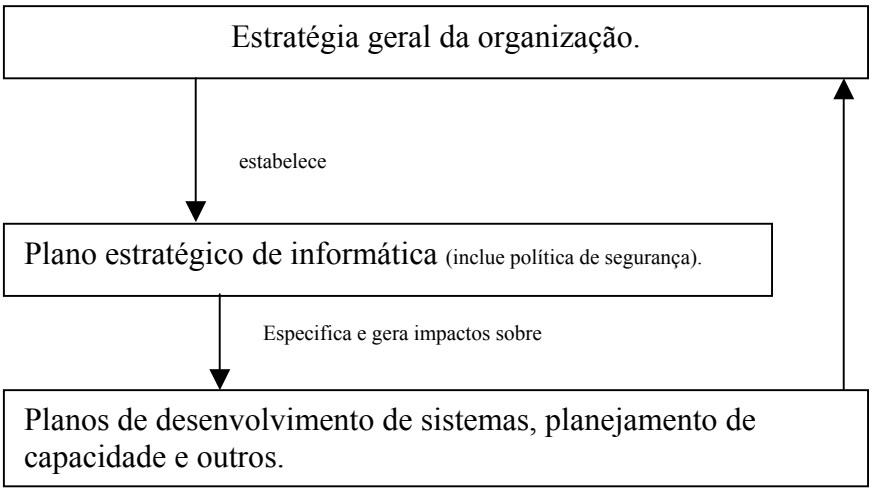


Figura 1. "Relacionamento entre estratégia da organização e planos de informática"

A política de segurança visa manter propriedades como confidencialidade, integridade e disponibilidade [6]. O público alvo que fica sujeito a política é formado por funcionários da empresa, fornecedores, clientes e outros usuários de forma geral.

[1] Auxiliam no restabelecimento do processamento dos sistemas críticos da organização, levando em consideração o estado decisivo de cada sistema e o prazo previsto para o seu restabelecimento, de modo que minimize eventuais perdas à organização, podendo estas, serem financeiras, jurídicas ou de imagem.

Buscando uma implantação mais segura, pode-se dividir o processo entre identificação dos recursos críticos, classificação das informações, definição dos objetivos de segurança a serem atingidos, análise das necessidades de segurança (identificação das possíveis ameaças, análises de riscos e impactos), elaboração de proposta da política, discussões abertas com os envolvidos, apresentação de documento formal à gerência superior, aprovação, implementação e revisão. O seguimento destas etapas facilitará a compreensão e execução do processo de implantação.

2.3 Ameaças

Qualquer ação que comprometa a segurança de informação da organização pode ser considerada uma ameaça [15]. Para se garantir a proteção de uma rede ou sistema é importante conhecer as ameaças e técnicas de ataque utilizadas pelos invasores, para então aplicar as medidas e ferramentas necessárias para proteção desses recursos. Sem o conhecimento desses fatores, toda a aplicação de mecanismos de proteção pode ser anulada, pois se existir algum ponto vulnerável ou protegido de maneira incorreta, todo sistema estará comprometido.

Os vírus geralmente são formados por seqüências de códigos inseridas em outros programas executáveis, de forma que, no momento em que esses programas são ativados, os vírus são executados. Sendo assim, uma vez ativo, o vírus pode infectar imediatamente outras partes do computador (outros programas, arquivos, disquetes e setores de disco) ou permanecer residente na memória do computador. Entre os tipos de vírus destacam-se:

- *Worms* - programas que podem rodar independentemente e trafegam de uma máquina a outra através das conexões de rede, podendo ter pedaços de si mesmos rodando em várias máquinas, um exemplo é o "*LoveLetter"*.
- Cavalo de Tróia - um programa que possuem uma função, mas que na realidade, executa outras funções. Análogos ao mito da história grega, os cavalos de Tróia modernos se parecem com um programa que o usuário gostaria de rodar (como um jogo, uma planilha eletrônica ou editor de textos). Enquanto parece estar executando o que o usuário quer, na verdade, o cavalo de Tróia está fazendo algo completamente diferente como, por exemplo, apagando arquivos, formatando discos ou alterando dados. Tudo o que

o usuário vê é apenas a *interface* adulterada do programa que ele queria utilizar. Quando o cavalo de Tróia é percebido, geralmente já é tarde demais. Normalmente os cavalos de Tróia são utilizados como veículos para vírus, *worms* e outras ameaças programadas. Mas não deve-se generalizar ameaças apenas em vírus, *worms* ou cavalos de tróia, outras formas devem ser lembradas.

Existem técnicas de invasão que podem gerar muitos problemas, como a de "*Flooding*", onde o atacante envia muitos pacotes em curto período de tempo, de forma que a máquina vítima fica sobrecarregada e começa a descartar pacotes (negar serviços) [8]. Poderia ser escrito um livro somente com técnicas de invasão, o qual não é o objetivo deste trabalho, mas não pode-se deixar de citar outros nomes como "*Sniffers*" e "*Scanning*", os quais são também formas conhecidas de invasão. Quanto ao primeiro *Sniffers* ou "farejadores", são programas que exploram o fato de o tráfego de pacotes das aplicações TCP/IP não usar nenhum tipo de cifragem nos dados. Já os *Scanning*- Internet, possuem o objetivo de procurar por serviços e falhas que possam comprometer uma máquina.

2.4 Mecanismos de Segurança

Os mecanismos de segurança são o conjunto de técnicas, procedimentos e algoritmos que quando usados adequadamente possibilitam a implementação e garantia de aplicação da política de autorização e autenticação de um sistema. Dentre alguns dos mecanismos que podem ser utilizados, tem-se a criptografia, a autenticação e o controle de acesso.

2.4.1 Criptografia

A arte de escrever ocultamente, assim alguns autores descrevem a criptografia, talvez tão antiga quanto à própria escrita, hoje é um dos métodos mais eficientes de se transferir informações, diminuindo a possibilidade de comprometimento do sigilo. Segundo [10], algoritmos criptográficos usam chaves para proteger os dados. Então utilizando as chaves, uma informação pode ser codificada através de algum algoritmo de criptografia, de

modo que, tendo conhecimento do algoritmo utilizado e da chave utilizada, é possível recuperar a informação original, fazendo o percurso contrário[8].

Com o aumento da capacidade computacional, hoje utiliza-se complexos esquemas criptográficos, que antes eram impraticáveis pela demora com os quais eram codificadas pequenas informações [1]. A criptografia pode ser dividida em:

Criptografia de Chave Simétrica e Criptografia de Chave Assimétrica.

2.4.2 Criptografia de Chave Simétrica

Esta é a criptografia tradicional, onde a mesma chave utilizada na codificação deve ser utilizada da decodificação. De acordo com [8], estes são exemplos tradicionais de algoritmos de criptografia utilizando chave simétrica: IDEA (*International Data Encryption Algorithm*), DES (*Data Encryption Standard*) da IBM e o RC2/4, da RSA *Data Security*. O problema dessa simetria é: como informar ao destinatário a chave para a decifragem de forma segura. No entanto, a criptografia simétrica é bastante eficiente em conexões seguras na Internet. Conforme [9], quando navega-se pela Internet e visita *sites* "seguros", onde geralmente são preenchidos dados sigilosos, comumente está se utilizando o SSL (*Secure Socket Layer*) que funciona usando primeiro a base criptografia assimétrica, para a troca de chaves de sessão e depois usa criptografia simétrica para acelerar o processo de cifragem e decifragem.

2.4.3 Criptografia Assimétrica

Algumas análises e estudos realizados tornaram possíveis algoritmos de criptografia utilizando duas chaves. Cifrando-se com a chave A, só seria possível a decifragem com a chave B, sendo a recíproca verdadeira.

Esta assimetria nos dá uma outra abordagem: a de chave pública e chave privada. Com duas chaves, não precisamos ficar presos a uma "troca" para o processo de decodificação [8]. Cada um poderá possuir sua chave pública e sua chave privada. Como o próprio nome já diz, a chave privada é de conhecimento único e exclusivo. Já a pública deve estar disponível a quem quiser lhe enviar informações cifradas. Como a cifragem / decifragem depende das duas chaves, caso se queira, por exemplo, mandar uma mensagem

cifrada, deve cifrá-la com a chave pública. Como dito anteriormente, a única chave que decifra esta mensagem é o par da chave pública, ou seja, a chave privada. Somente com uma chave privada se consegue ler a mensagem. Continuando o exemplo, caso se deseje mandar uma mensagem cifrada, primeiro deve-se conseguir uma cópia da chave pública e usá-la na cifragem. Somente uma chave privada poderá decifrar esta mensagem, e mesmo que a mensagem tenha sido interceptada, não passará de um conjunto de caracteres desordenados e sem significados.

2.4.4 Autenticação

Autenticação é a capacidade de garantir que um usuário é de fato quem ele diz ser, sendo assim, uma das funções de segurança mais importantes que um sistema deve fornecer [16]. Os mecanismos de autenticação podem ser divididos em quatro categorias:

- **Algo que se sabe** - O mecanismo mais utilizado é nome do usuário/senha, embora seja relativamente inseguro.
- **Algo que se tem** - Chaves de carro, cartões de banco 24 horas, e outros dispositivos físicos são mecanismos de autenticação que exigem a posse física de um dispositivo.
- **Algo que se é** - Impressões digitais, análise de retina e reconhecimento de voz são exemplos de mecanismos biométricos que podem ser usados.
- **Algum lugar onde se está** - Endereços de adaptador de rede e sistema baseado em Posicionamento Global via Satélite provêem informação de autenticação baseada na localização do usuário.

Senhas de acesso são métodos mais utilizados para a autenticação de usuários. Porém para garantir o seu uso adequado deve ser definida uma política de senhas, em que sejam criadas regras para a criação, troca e uso das mesmas. As regras definidas devem ser divulgadas a todos os funcionários e colaboradores da organização.

Uma outra moderna tecnologia está sendo bem difundida atualmente, a Biometria. Nos últimos anos muito se tem pesquisado na área de sistemas automáticos de verificação de identidade, baseados em características físicas do usuário [14]. Com o objetivo de aumentar a garantia em um processo de autenticação, e suprir deficiências de segurança de

senhas. Acredita-se que sistemas assim são mais difíceis de serem forjados, porém são mais caros. Os sistemas biométricos automáticos são uma evolução natural dos sistemas manuais de reconhecimento amplamente difundidos há muito tempo, como a análise grafológica de assinaturas, análise de impressões digitais e o reconhecimento da voz.

Hoje já existem sistemas ainda mais sofisticados, como os sistemas de análise dos vasos sangüíneos da retina. Um dos problemas enfrentados por esses sistemas é sua alta taxa de erro, em função das mudanças das características dos indivíduos com o passar dos anos, devido a problemas de saúde ou nervosismo, citando como exemplo impressões digitais[2], geometria da mão[3] e os sistemas de reconhecimento de voz, todos usados para controle de acesso, e que no último caso, em função de problemas na garganta, cordas vocais, ruídos no ambiente, podem ocasionar diversas falhas.

2.4.5 Controle de Acesso

O controle de acesso é a mediação das requisições de acesso a objetos (dispositivos, computadores, canais de comunicação, programas, informação) solicitados pelos sujeitos. Essa mediação é realizada pelo monitor de referência do sistema, responsável por permitir ou negar o acesso correspondente. O monitor de referência é o modelo conceitual, entidade abstrata responsável pelo controle de acesso definido por [16].

Segundo [5], o fato de um usuário ter sido identificado e autenticado não quer dizer que ele poderá acessar qualquer informação ou aplicativo sem qualquer restrição. É necessário implementar um controle específico restringindo o acesso dos usuários apenas às aplicações, arquivos e utilitários imprescindíveis para desempenhar suas funções na organização. O controle de acesso pode ser classificado em:

Controles de acesso físico e controle de acesso lógico. No controle físico tem-se a segurança de acesso, que trata das medidas de proteção contra acesso físico não autorizado, e a segurança ambiental, que trata da prevenção de danos por causas naturais. O controle de

[2] Sistema que compara a impressão lida com uma base de dados de impressões digitais de pessoas autorizadas.
[3] Sistema que mede a distância entre pontos na palma da mão, mas que pode ser facilmente alterado devido a problemas de peso ou artrite.

acesso lógico permite que os sistemas de TI (tecnologia de informação) verifiquem as permissões dos usuários que tentam utilizar seus serviços.

2.5 Conclusão do Capítulo

Com o crescimento da quantidade de dados que circulam no universo da informática, é percebível o surgimento de meios de segurança que buscam a proteção das informações, no sentido de manter a **confidencialidade** (sigilo da informação), a **integridade** (informações íntegras, corretas), e a **disponibilidade** (informação disponível).

Com o aumento da popularização da rede mundial de computadores, maior é a preocupação com a segurança, pois a Internet é hoje utilizada para acessar serviços, fazer *downloads*, compras, e se ocorrer um problema no sistema, isto pode provocar ausência/ insuficiência de matéria prima, suprimentos importantes, invasões e apropriações indevidas de conteúdos. A importância dos métodos utilizados para combater invasões e acessos não autorizados se destaca na sociedade insegura, que busca por meio de soluções, o resgate da confiança. Sendo assim é através do surgimento e aperfeiçoamento das tecnologias e políticas, que pretende-se melhorar a segurança dos dados e informações.

3 Distribuição de Documentos

Com o mundo digital em plena fase de desenvolvimento, novos negócios, tendências, e novas tecnologias passam a surgir nesta era da informação. Com toda esta evolução, a Internet começou ser vista como uma forma de expressão e um portal de um novo mundo [6], uma maneira de relacionamento entre as pessoas e de se fazer negócios.

3.1 E-commerce e E-business

Qualquer forma de transação de negócio na qual as partes interagem eletronicamente, ao invés de existir contato físico direto, são conhecidos como Comércio eletrônico ou "*e-commerce*" [49]. Na realidade essa nova forma de comércio utiliza os recursos tecnológicos da informática e da comunicação disponíveis para realizar operações tradicionais de compra, venda e distribuição de conteúdos de forma mais rápida e acessível para alguns casos.

Para que o potencial do comércio eletrônico seja aproveitado corretamente, é necessário que as soluções envolvam diversas áreas, desde processo de compra e venda, marketing, logística à segurança de sistemas de informação[47]. Pode-se considerar o comércio eletrônico um aspecto do *e-business.* No comércio eletrônico há uma venda da empresa para o consumidor final e no *e-business* não existe necessariamente uma venda, mas sim uma adequação dos sistemas da empresa por conveniência e disponibilidade a fim de aumentar os negócios existentes ou criar novos negócios virtuais [47].

Uma preocupação constante nestas negociações digitais é a segurança, por este motivo, grandes empresas como Microsoft e IBM buscam sempre novas tecnologias para garantir o sucesso do comércio digital. Um caso especial de comércio eletrônico é a venda eletrônica, no qual um fornecedor vende bens ou serviços para um cliente em troca de um pagamento, equivale em grande parte ao varejo eletrônico. Esta categoria tem tido um crescimento enorme com o advento da *www;* existem shoppings eletrônicos por toda internet oferecendo de tudo, desde bolos e vinhos a computadores, carros e livros sendo conhecido como B2C "*business to consumer*". Existem outros como: C2C "*consumer to consumer*", e nesta modalidade, uma organização comercial faz a intermediação entre

consumidores, geralmente pessoas físicas, que desejam comprar, vender ou trocar produtos ou serviços na Internet. Já o B2B "*business to business*" é o nome que se dá a transações comerciais entre empresas.

O "*peer-to-peer*", P2P ou fim a fim, é uma forma de troca de arquivos que imita a própria estrutura da Internet: em vez de manter os dados a serem trocados, estocados numa central única, como fazia o *Napster*[4] (tornando a central vulnerável a ataques), na estrutura P2P a matriz de arquivos está distribuída por todos os participantes. Então a tecnologia não cria uma relação usuário-central-usuário, no P2P todos os usuários são também mini-centrais.

Muitas empresas se utilizam destes tipos de *e-commerce* para se relacionar com seus fornecedores, fazendo pedidos, recebendo e pagando faturas e pagamentos, trocando dados e captando novos parceiros [44]. Entretanto, enquanto estes casos são de considerável importância econômica, eles são apenas alguns dos exemplos, de operações de negócios ou transações conduzidas via meio eletrônico. Com toda a variedade dos meios de transmissão disponíveis que encontra-se no mundo hoje, e as várias estatísticas disponíveis nos canais de comunicação, devemos salientar mais uma vez a importância da segurança, pois a mesma pode se tornar uma barreira tanto para consumidores quanto para parceiros. No mundo atual de dispositivos com e sem fio, a mídia digital contém um potencial ilimitado para comércio B2B (*business-to-business*) e B2C (*business-to-consumer*).

3.2 Categorias do E-business

Nesta seção são apresentadas algumas categorias existentes no *e-business*. Essas categorias são definidas pelo negócio a ser realizado na forma digital [47].

3.2.1 E-Auctioning

Os leilões digitais ganharam força na Internet, pois na forma tradicional os mesmos eram restritos a um local e a um determinado número de pessoas. Com a utilização da *Web,* qualquer pessoa pode participar dando seu lance. A variedade de objetos que são

[4] *Napster* é um *Software* totalmente *freeware*, onde você pode trocar músicas *MP3* com outras pessoas pela Internet sem enfrentar grandes dificuldades.

encontradas nos leilões é vasta, e pode-se encontrar desde uma simples caneta até um automóvel.

Com isso a pessoa não tem custo de locomoção para o lugar onde o leilão está sendo realizado, os lances feitos são registrados pelos leiloeiros e são finalizados em questões de segundos.

3.2.2 E-Banking

Esse tipo de serviço pode trazer comodidade para os clientes que através de um site podem acessar suas contas da mesma maneira com se estivesse em um caixa automático (*ATM – Automated Teller Machine*). Através do *site* é possível verificar saldos, extratos, realizar pagamentos, fazer transferências de conta e outras operações desejadas que o banco possa oferecer.

3.2.3 E-Directories

Esta categoria de *e-business* é representada pelos catálogos que tem como objetivo fazer com que determinado serviço ou produto seja encontrado facilmente. As listas telefônicas ou as listas amarelas são os exemplos mais comuns. Estas foram disponibilizadas na *Web* da mesma maneira que é possível ligar no serviço de informações de uma companhia telefônica e pedir o número do telefone de uma pessoa específica. No Brasil a empresa TIM oferece esse tipo de serviço, (http://www.listasdaqui.com.br no estado de Santa Catarina), no qual a busca da informação pode ser feita pelo nome do assinante ou pelo endereço e cidade.

3.2.4 E-Learning

O aprendizado feito pela Internet pode ser bastante útil considerando-se a velocidade com que as informações têm mudado atualmente. Como o mundo tecnológico evolui a cada dia, é necessário que haja um constante aprendizado. Existe também a possibilidade de aprender novos assuntos de maneira rápida através dos softwares que estão disponíveis na rede. Um exemplo típico desta forma de aprendizado são as aulas de inglês, que são oferecidas por algumas escolas.

3.2.5 E-Procurement

Esta categoria de e-business tem como objetivo reduzir os gastos das compras rotineiras de materiais que são importantes para o funcionamento da empresa, mas que não estão intimamente relacionados com os produtos e serviços oferecidos pela empresa em seu mercado. Um exemplo deste caso é uma metalúrgica, que embora não trabalhe na fabricação de papel, caneta, e borracha necessita destes materiais para o seu funcionamento geral.

O objetivo do *e-procurement* é diminuir a série de procedimentos para compras e os custos envolvidos.

3.2.6 E-Recruiting

Algumas empresas estão utilizando essa nova tecnologia para recrutar candidatos a determinadas vagas. O diferencial entre o recrutamento on-line e o recrutamento no mundo real é que os testes são feitos através da *web*. A empresa pede que o candidato acesse um determinado local com dia e horário pré-estabelecido. Com essa nova forma de recrutamento há vantagens tanto para empresas quanto para candidatos. Para a empresa, por que não há necessidade de agendar horários com todos os candidatos para entrevista; não é necessário reservar salas para a aplicação de provas, por exemplo. Para o candidato, ele tem a comodidade de não precisar se locomover até determinado local para tentar conseguir um emprego.

3.3 Conclusão do capítulo

As categorias de *e-business* citadas são alguns exemplos de negócios existentes na *web*, Todas podem de uma maneira ou de outra utilizar tecnologia de segurança para proteger os conteúdos digitais que estão armazenados ou trafegam na rede.

No futuro, provavelmente qualquer tipo de negócio conseguirá produzir uma forma lucrativa de negociação pela *web.* Isto acaba reforçando a crença no crescimento de tecnologias que necessitam proteger e liberar conteúdos digitais.

4 DRM – Digital Rights Management

O aumento de informações que circulam pela rede mundial de computadores gera uma ampliação considerável no comércio digital, gerando também o aumento de falsificações de produtos digitais. Por este motivo é cada vez maior a busca por modelos de "comércio digital de sucesso" [6], que mantêm os direitos de acesso em ambiente controlado.

Nesse contexto, o DRM (*Digital Rights Management*) vem tornando-se a tecnologia para gerenciar a segurança, o acesso, o uso e reprodução de arquivos digitais, seja on-line ou off-line, visando garantir que somente pessoas com acesso autorizado possam usar os produtos digitais [2]. Segundo [59], DRM é o processo de gravação, transmissão, interpretação, garantindo os direitos autorais e que tem como objetivo impedir o uso desautorizado e preservar a integridade da informação digital. Neste sentido existe a necessidade de se padronizar a maneira como ocorre a comunicação dos direitos com os sistemas que são capazes de garantir os direitos definidos.

DRM permite criar novos modelos de negócios, canais de distribuição adicionais e novos mercados. Os modelos de negócio são considerados um dos maiores recursos que estão sendo trabalhados na distribuição digital, e são potencialmente os maiores atrativos para os consumidores [20]. Alguns dos exemplos destes novos modelos de negócios são [27]:

- Vendas por etapas "fatias": Um exemplo típico deste caso é a de venda dos capítulos de um livro, no caso dos *e-Books*.
- Ofertas promocionais: Amostras grátis compreendem este exemplo, ou seja, é determinado um tempo limitado de acesso em um documento, ou *software*.
- Superdistribuição: Usuários que distribuem documentos (músicas, filmes etc) para outros usuários.

DRM (*digital rights management)*, inicialmente enfocou seus estudos em métodos de segurança, como um dos meios para resolver o gerenciamento de propriedade intelectual, sempre procurando uma maneira de proteger os conteúdos e de limitar suas distribuições. Esta fase marca a primeira geração DRM, onde a proteção da propriedade intelectual destacou-se como ponto alto.

Considera-se que o gerenciamento de direitos digitais está atualmente na segunda geração, que busca garantir a descrição, identificação, o comércio, a proteção e monitoramento das informações, seguindo todos os formulários de permissões de direitos, restrições e requerimentos, incluindo o gerenciamento dos direitos proprietários [26].

4.1 Conteúdo digital

A mídia impressa, o rádio, a televisão entre outras, começam a perder o espaço para os conteúdos digitais [44]. O papel vai cedendo lugar a impulsos eletrônicos (*bits*), que podem ser transmitidos de forma rápida e também atualizados instantaneamente nas telas dos computadores, gerando tipos de conteúdos digitais como: gráficos, imagens, animações, áudio, vídeo ou outros dados.

Embora essa transformação nos meios de comunicação esteja no início e a maioria das pessoas ainda não possuam muita interatividade com o meio digital, as mídias tradicionais já perceberam que estão diante de um quadro novo e que é preciso investir em novas tecnologias para acompanhar o ritmo das mudanças.

No passado, as empresas não tinham alternativa senão aceitar os atrasos e os custos altos embutidos na distribuição de documentos e na busca por informações importantes. Hoje tudo isso muda garantindo acesso imediato às informações necessárias para tomar decisões importantes, direcionar os processos do negócio e atingir resultados.

A era digital cria um novo paradigma para transmissão de documentos, simplesmente com um "*browser*", o usuário pode acessar e exibir as páginas individuais de relatórios, bem como outros conteúdos digitais criados por aplicativos comuns de uma empresa [37]. Essa verdadeira explosão do conteúdo digital tem várias origens: documentos, arquivos médicos, imagens de satélite, raios-X, vídeo, música, arquivos de voz e conferências digitalizadas. Entre os conteúdos mais conhecidos encontram-se as

músicas em formato "*MP3"* [5] e os livros eletrônicos (*e-books)*. Essa expansão aumenta a facilidade com que as informações digitais podem ser reproduzidas e distribuídas tornando a segurança de materiais com direitos autorais uma necessidade indispensável. A cópia ilegal de filmes, músicas ou livros não infringem apenas os direitos dos produtores, mas também os desencoraja fortemente a publicá-los.

Uma pesquisa realizada pela *Accenture* [37], uma companhia de consultoria tecnológica e administração global, motiva uma boa perspectiva de mercado de produtos digitais, como música, vídeo e livro eletrônico, nos Estados Unidos. Segundo a pesquisa, mais de US$ oito bilhões serão movimentados somente naquele país até 2005, assim distribuídos: US$ 3,2 bilhões no mercado de música, US$ 2,3 bilhões entre os consumidores de *e-books* e US$ 3,1 bilhões nas negociações de vídeo. Sendo assim, o avanço tecnológico vai criando uma nova sociedade, baseada na disseminação rápida e ampla dos conteúdos digitais.

4.1.1 Segurança de conteúdo e Direitos Digitais

A segurança de conteúdo tornou-se um elemento chave para o desenvolvimento da rede e de aplicações que por ela hoje circulam [15]. As organizações agora enfrentam um desafio sem precedentes: aproveitar ao máximo todo o potencial da Internet, enquanto minimizam os riscos de segurança, produtividade e competitividade [31]. Para vencer este desafio, as empresas precisam de produtos e serviços que as ajudem a proteger com segurança e eficácia seus ambientes de computação e seu conteúdo digital.

Virtualmente, todas as formas de conteúdo digital incluindo livros, vídeo games, música e software, agora estão disponíveis para distribuição digital. Outras informações importantes em formato digital, tais como relatórios financeiros, registros médicos, contratos e documentos contendo informações confidenciais ou sigilosas, devem ser distribuídas de forma segura dentro e fora de uma organização com proteção de direitos para impedir a utilização não autorizada. Atualmente os direitos autorais e a origem de dados são freqüentemente perdidos em virtude da facilidade de disseminação da

[5] *MP3* são arquivos de áudio em formato de compressão (como .zip). As siglas *MP3* representam o nome Mpeg 1 *Audio Layer* III.

informação via redes e pela falta de controle, indexação e catalogação deste bem digital [20].

Sendo assim, as empresas buscam soluções automatizadas e inteligentes que lhes permitam avaliar a sua vulnerabilidade, controlar o acesso e proteger a sua rede, seu ambiente computacional e sua equipe.

Também é muito importante conhecer os direitos que norteiam as informações encontradas na *Web*. A tecnologia trouxe um potencial enorme e atualmente é muito mais fácil duplicar com exatidão vários tipos conteúdos e materiais [44]. Este é um dos motivos que mais tem gerado discussões a respeito da eficiência e do cumprimento das leis hoje vigentes. Há pouco tempo tudo era abstrato e restrito, então com a propagação da internet, tudo passou a ser muito mais visível e de fácil acesso, podendo ser obtido, reproduzido e comercializado sem maiores dificuldades [34]. Entretanto, ainda é necessário ter permissão para utilizar conteúdos materiais protegidos pelos seus Direitos [25].

Direito nada mais é do que a ciência que estuda normas para disciplinar as relações sociais, descortinando assim leis capazes de impor limites a determinadas condutas [53]. Este conceito também é empregado para o termo direito digital, o qual usufrui dos mesmos objetivos mas de forma digitalizada, ou seja, leis e normas são representadas e impostas através de *bits* [53] .

Os direitos digitais são formas que empresas e autores encontraram para proteger seus produtos. Muitas vezes, estes direitos acabam beneficiando somente o fabricante ou o distribuidor do conteúdo. Por esta razão, os consumidores devem possuir o direito de compartilhar suas músicas, vídeos e outros conteúdos digitais que tenham adquirido, entre seus aparelhos de computador. Observa-se então, a necessidade de desenvolver um modelo de aplicação, que permita que o usuário possa realizar procedimentos deste nível com segurança.

Proteger os direitos autorais também é uma forma de direito digital. A proteção segundo a Lei Nº 9.610, de Direitos Digitais Autorais[6] [56], começa quando um trabalho original é apresentado de forma tangível e bem definida, seja através de uma partitura musical, de páginas de um livro, de um filme, ou outros meios. Muitas pessoas registram direitos autorais formalmente para se proteger contra possíveis violações. De acordo com [30], a utilização de avisos tradicionais (por exemplo, o sinal ©) ajudam a reforçar a propriedade intelectual. Existem também outras tecnologias que possibilitam o gerenciamento de direitos digitais como o DRM (*Digital Rights Management*). Além destas formas de proteção, devem-se monitorar novas iniciativas ou leis governamentais que possam influenciar os direitos digitais sobre materiais e conteúdos digitais.

4.1.2 Direitos digitais e suas Considerações

Um dos fatores tecnológicos para o sucesso da tecnologia DRM é a aceitação do consumidor, sendo assim, é importante transformar o gerenciamento dos direitos digitais em tecnologia sólida e de confiança [20].

O termo "direito digital" denota os direitos que um consumidor tem de usar e acessar um conteúdo específico, isto inclui direitos de assinatura, direitos para jogar ou ver peças individuais de um conteúdo, direitos para acessar conteúdo de vários dispositivos, direitos para redistribuir conteúdo. Por que uma pessoa deve pagar por um pouquinho de bits, ao invés de pagar por um cd físico? A resposta desta questão pode ser vista de diferentes formas, e uma delas é que, comprando bens digitais e os direitos associados, eles podem utilizar o conteúdo em implementações de algumas aplicações, onde fornecem várias formas de desfrutar o mesmo, de uma maneira conveniente e de confiança como o que eles tem no mundo físico. Tudo isto inclui a possibilidade de "jogar" ou (tocar) música digital nos vários dispositivos. Sendo assim, a portabilidade dos direitos digitais dentre várias plataformas, PCs, dispositivos eletrônicos, telefones sem fios, se faz de suma importância [20]. Outra necessidade também é o projeto dos mecanismos para cópia de segurança dos direitos digitais, pois podem ocorrer falhas de hardware ou até mesmo a

[6] Os Direitos digitais Autorais protegem a expressão de uma idéia, um conceito, ou um pensamento em uma forma concreta - como um vídeo, ou livro - e não uma idéia abstrata, um conceito, ou um pensamento.

compra de um novo computador. Um exemplo seria a substituição de um servidor de licenças do lado do fornecedor.

Uma das ferramentas para se ter portabilidade e possibilitará recuperação de direitos digitais é um "*locker* de direitos". Estes servem como um depósito central dos direitos digitais para tudo aquilo que o consumidor tem adquirido. Estes servidores centrais de direitos podem ser acessados e usados por múltiplos dispositivos. O desafio do Locker de direitos, está em ligar direitos digitais a uma pessoa, e não somente a um dispositivo [20].

4.2 Visão de uma arquitetura DRM

Este modelo de referência da arquitetura DRM proporciona uma visão genérica de como alguns dos sistemas atuais funcionam. A maioria de sistemas da grade comercial de DRM, incluindo aqueles usados para controlar o uso de documentos, e *Downloads* de arquivos multimídia, seguem a arquitetura geral apresentada na figura 2.

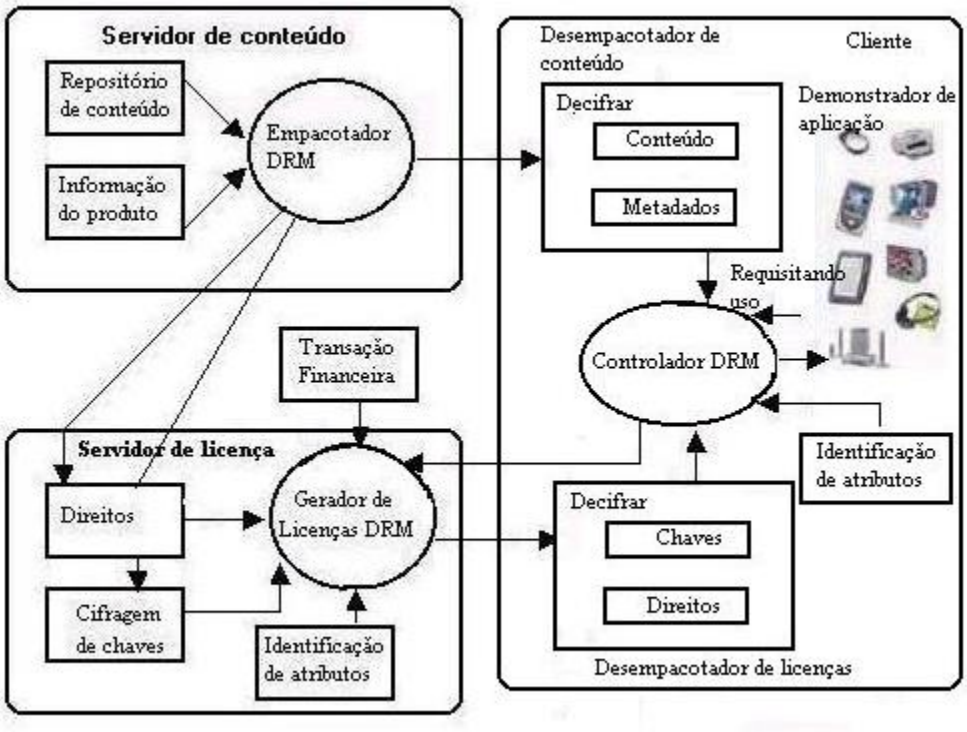


Figura 2."Organização básica de uma arquitetura DRM" [43, 57].

A obtenção do conteúdo pelo usuário, pode ser considerado o primeiro passo onde o usuário pode receber o conteúdo como transferência de arquivo através de protocolos, ou também requisitando diretamente para um servidor de arquivos. Logo após o usuário tenta usar o conteúdo de alguma maneira, sendo que o cliente de DRM determina, quais as políticas limitadas ao pacote (conteúdo) e/ou implícitas no empacotamento.

Neste passo o cliente do DRM faz a solicitação de direitos para usar o conteúdo. Se o pacote de licença contendo as credenciais das autorizações necessárias não podem ser encontradas na máquina do usuário, ou está com o prazo expirado, faz-se uma solicitação do usuário incluindo o contexto de uso para um servidor de licença. O servidor de licença verifica a identificação submetida do cliente ou atribui credenciais, a partir de uma identidade ou banco de dados de atributo. O servidor de licença também analisa os direitos especificados acima (regras) para o item deste conteúdo. Caso o cliente deva pagar pelo conteúdo, uma transação financeira acontece.

Os conteúdos do pacote de licença são montados: a especificação de direitos, vários identificadores ou atributos, informação de revogação, chaves de criptografia para o conteúdo, tudo específico para o conteúdo e contexto de uso. A licença é seguramente empacotada (incluindo informação de autenticação) e transferida para o cliente. O cliente usa a licença para abrir o conteúdo de uso particular solicitado, e o conteúdo é recebido do modo como foi solicitado.

No modelo da figura 2, foi demonstrado que as interações entre o cliente do DRM e o gerador de licenças DRM, são feitas usando mensagens que definem os direitos (formas de interação), que devem ser estipulados empregando o vocabulário definido pela linguagem de expressões de direitos conhecida como REL (*rights expression language*).

4.2.1 Organização de uma Estrutura DRM

Em determinados sistemas a restrição de acesso é realizada através de um RAS (*Remote Access Server*) o qual provê senhas e controle de autenticação. Após realizar a autenticação o RAS verifica o que se tem direito de acesso. Na seqüência desta operação o conteúdo é transferido e não há nada no outro *host* (usuário do sistema) que proíba o uso

não liberado das informações [31]. Uma das soluções DRM é fornecer uma autorização juntamente com uma proteção, que tem a finalidade de solucionar este problema.

Os Metadados são informações que acrescem aos dados e que têm como objetivo informar-nos sobre eles. Considerando este conceito pode-se concluir que as informações de direitos devem ser colocadas desta forma no próprio conteúdo ou separadas do conteúdo original.

Quando o direito está dentro do conteúdo, as informações de direitos estão conectadas a ele, então os direitos serão sempre os mesmos e não serão sensíveis ao contexto. Qualquer mudança é dificultada por este fato. No segundo caso, quando os direitos são mantidos separados dos metadados sobre o conteúdo, o mesmo conteúdo pode ser distribuído unicamente de diversas formas possíveis atualmente, e alterações tornam-se mais viáveis [22].

Existem também alguns sistemas que possuem quase o mesmo princípio, mas com dois servidores. Tendo-se um servidor de *download* e outro de licenças, pode-se então dividir a estrutura em 2 etapas distintas, uma de *download* e outra da obtenção de licenças [24]. A proteção e disponibilização do conteúdo podem ser consideradas a primeira etapa; nesta fase ocorre o "empacotamento" ou criptografia do conteúdo já em formato digital. Aqui se determinam ainda, quais serão as regras para seu consumo, é oferecido um *download* promocional, ou determina-se que aquele conteúdo poderá ser acessado apenas por algumas vezes ou ter um tempo de vida de um número pré-determinado de dias. Depois de estabelecida a política de consumo, o conteúdo será disponibilizado em um servidor de *download.* Uma cópia dos direitos e requerimentos para licenciamento, ficariam em um servidor de licenças que seria acessado no segundo momento.

Na segunda fase ocorre o consumo do produto; o usuário busca o conteúdo de seu interesse e efetua o *download*. Neste ponto, o servidor de licenças é acessado e automaticamente envia pela rede as informações necessárias para liberar a licença: informações sobre o usuário, número do cartão de crédito, ou simplesmente uma senha. A seguir é realizado o *"download"* de um número de série que possibilitará consumir o conteúdo. No caso do usuário copiar o conteúdo, incluindo o número de série, e remeter para alguém, quando houver a tentativa de consumi-lo novamente, será efetuada a conexão

com o servidor de licenças e serão enviadas as informações necessárias que podem ou não liberar o conteúdo.

4.2.2 Facilidades de Uso

A facilidade de uso é outro fator crucial para alguns produtos de DRM. Infelizmente a usabilidade tem sempre sido um dos maiores desafios em segurança de computadores, DRM não é exceção [20]. Isso porque usuários honestos podem ficar aborrecidos com as restrições impostas pelas medidas de segurança [37].

Facilidade de uso foi um dos problemas encontrados por produtos DRM da primeira geração. Já na segunda geração os produtos começaram a investir um pouco mais em *interfaces* de fácil nível e mecanismos intuitivos, para apresentar e oferecer os bens digitais. Além disso, mecanismos de autenticação do usuário são basicamente indispensáveis, para controlar o acesso e armazenar os direitos.

O DRM vem procurando trabalhar a segurança e a facilidade de uso sem restringir muito os direitos dos usuários, pois a restrição excessiva acaba atrapalhando o crescimento da tecnologia. Esta ameaça dificulta muito sua expansão, pois em muitas das vezes os usuários abandonam um determinado produto, devido sua alta exigência de informações. Conforme [41], construir uma plataforma de interoperabilidade é uma excelente maneira para se conseguir as facilidades de uso e conveniência.

4.3 Tecnologias Existentes

Na busca da sobrevivência e procurando investir no futuro próximo, sabendo que podem influenciar nos padrões, as editoras buscam a entrada no mercado do gerenciamento dos direitos digitais dos *e-books*. Os livros digitais, ou *eBooks* são livros, ou publicações, em formato digital, que podem ser "descarregados" para um computador e lidos com ajuda de um software especial (*e-book reader*)[7]. Mas as editoras estão receosas com a questão da

[7] *E-book reader* é um software gratuito, disponível na *Web*, e nos inúmeros *CD-ROMs* que todos os meses as revistas colocam no mercado. O *e-book reader* tem de estar instalado no computador para que a leitura do *e-book* seja possível logo após o seu *download*. Alguns exemplos são Adobe Acrobat eBook Reader ou Adobe AcrobatReader.

segurança. Neste sentido, o DRM tenta assegurar às casas publicadoras, editores e autores, a proteção e segurança na transmissão e repasse de direitos autorais de obras, através da determinação de especificações de como os usuários poderão acessar os seus documentos virtuais, se apenas poderão ler os documentos em tela ou se estariam disponíveis para impressão, e quantas vezes poderiam ser impressos.

Apesar de tantas normas, o gerenciamento de direitos digitais ainda encontra-se em fase de desenvolvimento [19]. Entre as preocupações encontram-se a questão da integridade dos livros e a carência de uma ferramenta que verifique se a obra não foi modificada. Neste caso o usuário teria que comparar a obra original com a versão digital, ou confiar na fonte de onde esta obra foi obtida. Sendo assim, os mais diversos e modernos mecanismos de proteção para direitos autorais, tendem a confiar na expansão de novas tecnologias.

4.3.1 Marca d'água "Watermarks"

Uma das abordagens que tem se mostrado mais promissora para controlar esta disseminação indiscriminada de informações é a inserção de um código digital de identificação/segurança no conteúdo digital. Após a difusão ou publicação do conteúdo digital, este código pode ser recuperado, permitindo assim o reconhecimento da origem das informações. Segundo [42], esta abordagem está associada à técnica milenar denominada steganografia, a qual visa inserir uma informação extra de forma imperceptível aos olhos menos atentos.

Este código digital é denominado marca d'água, e as técnicas de inserção de marcas d'água encontram inúmeras aplicações relacionadas ao controle e à difusão de conteúdo digital, proteção de *"copyright"*, rotulação de cópias, proteção contra cópias, monitoramento de difusão, autenticação de dados, junção de dados, segurança de dados médicos ou legais, transmissão secreta de informação, etc. Os requisitos a serem satisfeitos no desenvolvimento de técnicas de inserção de marcas d'água dependem da aplicação. Em geral, as seguintes propriedades devem ser ponderadas [29]:

• Transparência: a inserção da marca d'água não deve afetar a qualidade da informação original. Além disso, marcas d'água devem geralmente ser imperceptíveis;

• Tamanho: quantidade de informação associada à marca d'água;

• Robustez: resistência da marca d'água a possíveis ataques incidentais (distorções introduzidas por ruído, compressão com perdas, e filtragem), ou a ataques propositais que visam alterar, apagar ou substituir a marca d'água;

• Segurança: A marca d'água deveria ser detectável somente com o conhecimento de uma chave, independente do conhecimento do processo de inserção; e,

• Necessidade ou não de conhecer a informação original na detecção da marca d'água.

Com a crescente digitalização de informações sensíveis e de grandes acervos (bibliotecas, e museus,), o domínio da tecnologia de inserção de marcas d'água passa a ter grande importância. Entretanto, apesar de todos os esforços dispendidos nos últimos anos para a concepção de métodos eficientes para a inserção e detecção de marcas d'água em conteúdos digitais, ainda não chegou–se a técnicas que sejam insusceptíveis a todos os tipos de ataques possíveis ou que satisfaçam simultaneamente a todos os critérios desejáveis. De acordo com [30], os conteúdos sem *watermarks*, somente com a criptografia tradicional estão sendo considerados desprotegidos. As empresas estão considerando o gerenciamento de direitos digitais essencial para seu sucesso, “Os selos e as editoras apostam no êxito em torno dessa tecnologia” [29].

4.3.2 DOI - *Digital Object Identifier*

Dentro da expectativa dos envolvidos com conteúdo para *eBooks*, também está nascendo um grande e novo paradigma que envolve a segurança de objetos digitais na Internet, o DOI (*Digital Object Identifier* ou Identificador de Objeto Digital). O mesmo consiste num sistema de identificação numérico para conteúdo digital, uma espécie de ISBN para os livros eletrônicos e para documentos em geral [38].

O sistema DOI é um método desenvolvido pela Associação de Publicadores Americanos (AAP), para prover a base administrativa de conteúdo digital. Ele fornece a publicadores e membros da Internet, identificadores e nomes sem igual para seus os objetos digitais (*e-books*, imagens, arquivos e músicas). Implementado junto a sistemas de segurança, o DOI é concebido como um “número”, mas não tem um sistema de codificação pré-definido e também não traduz ou “analisa gramaticalmente” este número. Ele emite

nomes e informações a produtos e armazena dados sobre os seus atuais detentores e donos (associações profissionais e empresas de tecnologia). Então, atribui um número único e exclusivo, o identificador de objetos digitais, a todo e qualquer material publicado.

O DOI surgiu para, de um lado, auxiliar no pagamento de direitos autorais através de um sistema de distribuição de textos digitais e, de outro, prover meios para localizar e acessar materiais na *web* [39]. O projeto também faz parte de um esforço muito mais amplo para tornar o conteúdo da rede mundial mais fácil de localizar e acessar. Os livros só começaram agora a entrar nesse sistema, mas já existem três milhões de DOIs em uso, dando referências cruzadas ativas sobre publicações acadêmicas e profissionais on-line[8].

O número DOI consiste de duas partes: primeiramente o prefixo ou uma raiz que identifica o publicador do documento, e a segunda parte consiste em um sufixo determinado pelo publicador do documento, ou editora, que fica todo à direita do prefixo, que é único e exclusivo para cada obra. Por exemplo:

- "10.5555.1 / + ISBN"

A IDF (*International DOI Foundation* ou Fundação Internacional de DOI, órgão gerenciador baseada em Genebra) nomeia a raiz DOI e provê a certeza que cada raiz é diferente uma da outra [38]. Os livros, por exemplo, provavelmente utilizarão como sufixo o número que já consta do ISBN - *International Standard Book Numbers* (sistema internacional de catalogação de livros). Quando um programa navegador encontra um número DOI, utiliza o prefixo para encontrar o banco de dados da editora e ali acessa as informações relativas ao livro, que podem incluir os dados do catálogo, exceto resenhas e *links*. A editora pode atribuir números DOI a partes dos livros, assim poderá vender capítulos isolados, para serem obtidos pela internet ou combinados com outros materiais, formando pacotes para cursos universitários ou livros especiais para serem impressos a pedido [38].

4.3.3 O Sistema Handle System e DOI

A tecnologia de base, chamada *Handle System* (algo como Sistema de Manipulação) foi desenvolvida por um órgão financiado pelo governo americano, o CNRI - *Corporation*

[8] Demonstração em www.crossref.org.

for National Research Initiatives. O presidente da CNRI, Robert E. Kahn, um dos criadores da internet, define a missão desse órgão como a de "reconceitualizar a rede, passando da movimentação de lotes de dados para a administração das informações".

Os identificadores DOI são registrados no servidor central na IDF, através do *Handle System*, que é projetado para recorrer a documentos de Internet pelas suas *URLs* (endereços) ou local físico em um servidor [39]. Quando um arquivo digital tiver um DOI associado, o *Handle System* dirige um pedido para o arquivo do dono do direito autoral, independente de seu local físico, garantindo assim o registro de direito no repasse de documentos. Este sistema ainda não chegou no Brasil, mas já está sendo implantado em algumas soluções DRM, como a usada na venda do *e-book* de João Ubaldo Ribeiro[9]. Sendo assim o sistema o DOI já é considerado uma parte do DRM, e faz com que a tecnologia evolua cada vez mais no mercado dos conteúdos digitais[40].

4.4 Certificados e Licenças

A tecnologia DRM vem procurando padronizar regras e opções de como formular uma licença através dos certificados, utilizando os modelos de negócios para efetuar uma operação determinada pelo usuário.

As licenças geralmente estipulam o que o usuário pode fazer e por quanto tempo, estabelecendo questões como: pagamento, identificação do usuário, e em qual dispositivo aquele conteúdo pode ser utilizado. O certificado atesta e garante quem é o usuário, ou seja, certifica-se se o usuário é quem ele realmente está dizendo que é.

[9] João Ubaldo Ribeiro, primeira obra e escritor brasileiro a lançar um e-book "Miséria e Grandeza do Amor de Benedita", Plataforma: PC/Windows, Editora Nova fronteira, PSI Net, Tribal e Image Technology - E-book (Edição Eletrônica) , 2000, SP.

Com a proliferação dos *e-Books*, as editoras e distribuidoras ficam ainda mais exigentes quanto à qualidade e garantia de suas certificações e licenças, então, a emissão de certificado é considerada um ponto crucial para a distribuição de um determinado produto.

Nesta sessão foram descritos alguns exemplos de ferramentas utilizadas pela tecnologia DRM, que podem ser implementadas em diferentes modelos de aplicações para a distribuição do conteúdo digital de forma segura e eficaz.

4.5 Sistemas que Utilizam DRM

Notavelmente cresce a demanda de usuários que procuram sistemas compostos por DRM; pessoas físicas ou jurídicas buscam soluções que possam garantir a segurança na transmissão de suas informações [44]. *Sites* de comércio eletrônico cada vez mais iniciam investimentos em seus sistemas, e começam a desenvolver novidades para não baixarem suas taxas de acesso. Assim como é notável o crescimento de usuários exigentes, é também importante salientar o aumento gradativo de sistemas seguros, esta evolução dos sistemas vai expandindo conforme os conteúdos digitais estão sendo requisitados no mundo digital.

4.5.1 eLocker

O *eLocker* é um sistema completo para operações de venda de conteúdo digital pela Internet[10]. Nele o cliente prepara o arquivo para distribuição, protegendo-o segundo as regras para licenciamento, e ao tentar reproduzir o seu conteúdo, o consumidor é direcionado para o sistema de *e-commerce eLocker*, onde escolhe a forma de pagamento desejada, entre várias disponibilizadas, e no final do processo recebe a licença de acordo com as regras definidas no momento da proteção do arquivo.

O envio da licença é feito de forma rápida e bastante descomplicada, basta que o usuário utilize uma das várias formas de pagamento oferecidas e disponibilizadas pelo sistema, de modo simples e seguro, utilizando o que há de mais moderno no que se refere a transações de *e-commerce* no Brasil. O *eLocker* pode auxiliar *sites* de modelos de negócios a distribuir e vender seu conteúdo *on-line* de diversas maneiras diferentes:

[10] www.locz.com/elocker/elocker.pdf

- Controlando a distribuição de vídeos pela internet no modelo *"pay-per-view",* podendo ser utilizado para exibições de filmes, vídeos de treinamento, shows ao vivo, cursos on-line, entre outros;

- Controlando a distribuição de arquivos de texto, como manuais, livros *(e-books)* e material didático em geral. Pode-se, neste caso, impedir que um determinado arquivo seja impresso ou mesmo cobrar taxas diferenciadas pela quantidade de impressões que o usuário terá direito na hora que adquirir uma licença; e,

- O sistema pode também controlar a distribuição de arquivos de áudio, licenciando, por exemplo, *áudio - books* ou até mesmo, faixas de música.

O *eLocker* é uma ferramenta para proteger os arquivos que serão distribuídos pela internet por outros *web-sites* ou por qualquer outro meio digital, como *CD-ROMs e email.* Os usuários do *eLocker*, criadores ou distribuidores de conteúdo (*content providers)*, têm acesso a um sistema completo de gerenciamento dos arquivos protegidos que vão desde a cifragem (proteção) do arquivo até a cobrança *on-line* do usuário final. Para proteger os arquivos o usuário precisa simplesmente ter o arquivo fonte preparado para ser visualizado pelos consumidores. O processo é feito em apenas quatro passos:

Passo 1: O usuário faz o "*upload"* deste arquivo para o sistema, ele pode fazer o "*upload*" de um arquivo sozinho ou mesmo de um lote de arquivos.

Passo 2: O usuário seleciona quais dos arquivos disponibilizados pelo sistema ele quer proteger.

Passo 3: Depois de selecionado o arquivo, é necessário que o usuário preencha o formulário de licenciamento. Neste formulário é decidido qual a política de licenciamento que será usada, isto é, é decidido o que o consumidor poderá fazer com o arquivo e quanto ele pagará para cada opção. Por exemplo, ele pode definir que seu arquivo texto pode ser comprado por R$ 5,00 para ser impresso duas vezes, e que também pode ser comprado por R$ 20,00, e o cliente pode imprimir seu arquivo dez vezes.

Passo 4: O usuário faz o *download* do arquivo, isso é, ele transfere o arquivo do servidor para seu computador. A partir daí, o "*content provider*" está com seu arquivo protegido, e pode distribuí-lo de diversas formas diferentes para o consumidor final. Um fator interessante é que mesmo depois do arquivo ser distribuído pela rede, sua licença pode

ser alterada pelo *site*, sem a necessidade de re-proteger o arquivo. Um exemplo disto pode ser uma música que foi licenciada da seguinte maneira:

Música “nome da música”

-Ouvir uma semana - R$ 1,00

-Ouvir um mês - R$ 2,00

Pode ser que depois de um mês, seja necessária uma alteração no preço, ou mesmo a alteração na política de licença. Por exemplo, alterar a licença para:

-Ouvir um dia - R$ 0,40

-Ouvir uma semana - R$ 2,00

-Ouvir um mês - R$ 8,00

Para fazer essas alterações basta que o usuário clique na licença que foi criada e altere os padrões. No mesmo instante os valores ficam atualizados para todos os arquivos distribuídos de qualquer maneira e por todo o mundo. Os usuários do sistema vão poder acompanhar todas as transações relacionadas com seus arquivos. É importante ressaltar que uma licença é dada para uma determinada máquina, o que o consumidor compra é o direito de acessar aquele arquivo de uma máquina e não de qualquer máquina.

Se o consumidor distribuir o arquivo licenciado para outras pessoas, o arquivo estará protegido da mesma forma, e cada consumidor terá que comprar novamente o arquivo. Ou seja, as distribuições dos arquivos protegidas deixam de ser um problema de distribuição desordenado, ao contrário, passa a ser uma forma de distribuição natural dos arquivos de uma forma controlada pelo *eLocker*, pois todos os consumidores terão que comprar o arquivo, fazendo com que todas as transações fiquem guardadas no sistema.

4.5.2 O IBM EMMS (Electronic Media Management System)

De acordo com [58], o EMMS fornece uma base independente da indústria para a entrega de recursos digitais que cria novos modelos de negócios, permite a flexibilidade do DRM (*Digital Rights Management*) e ajuda a proteger os recursos em todo o seu ciclo de vida. O EMMS consiste em vários componentes principais que interagem para fornecer aos proprietários de conteúdo, negócios, varejistas e consumidores um conjunto exclusivo de

soluções para suas necessidades de distribuição digital [40]. O EMMS tem os seguintes componentes:

O IBM EMMS *Content Preparation* SDK (*Software Development Kit*), *Clearinghouse Program* e *Client* SDK. Quanto ao *Content Preparation,* este é que integra recursos DRM em aplicativos verticais ou personalizados, específicos de um formato de conteúdo ou requisitos industriais. O *Clearinghouse Program* fornece funções de DRM e atua como um ponto de controle central para gerenciamento, autorização e relatório de transações. Ele verifica pedidos de licença, emite licenças que permitem que usuários finais acessem o conteúdo entregue em formatos suportados pelo EMMS, e fornece informações que podem facilitar pagamentos. Já o C*lient* SDK (*Software Development Kit*) permite que parceiros de negócios desenvolvam aplicativos clientes que fazem *download* ou transferência, utilizam e gerenciam conteúdo em um ambiente protegido contra violação, de acordo com direitos digitais especificados pelos proprietários de conteúdo. São fornecidas *interfaces* protegidas que ajudam a controlar a transferência de conteúdo, os metadados e os direitos digitais em formatos específicos dos dispositivos de recepção.

4.6 Conclusão do Capítulo

Este capítulo descreveu o que é a tecnologia DRM e sua estrutura de funcionamento, apresentando também alguns de seus elementos que contribuem para a segurança digital. A descrição de conceitos e pesquisas realizadas sobre direitos digitais, arquiteturas, sistemas que utilizam DRM e tecnologias como *watermarks* e DOI, buscam formar uma compreensão geral sobre *digital rights management*.

5 Trabalhos Correlatos

Dentre as pesquisas realizadas na área de DRM, poucos trabalhos conseguem demonstrar e esclarecer métodos ou padrões que possam ser utilizados na formação de uma padronização DRM. Observa-se muito a preocupação em manter o mínimo possível de informações ao lado do cliente, e todas que estiverem devem estar de forma protegida, com o intuito de dificultar ao máximo a distribuição ilegal destas informações. Os estudos realizados também buscam destacar fatores considerados relevantes na construção de uma estrutura ou arquitetura DRM. De acordo com [24], entende-se por arquitetura DRM, qualquer conjunto de elementos que juntos e interligados possam contribuir para a formação de uma solução na área de *digital rights management*.

O protótipo desenvolvido neste trabalho, demonstrado no capítulo sete e descrito em três publicações, oferece entre suas características e diferenciais, uma solução no armazenamento das informações, estas são mantidas cifradas e "escondidas" no disco do cliente. A decifragem dos dados ocorre somente no momento em que o *plug-in* abre o conteúdo, para dificultar ainda mais, foi elaborada uma extensão para o arquivo, onde somente o *software* gerenciador reconhece. Ainda como diferencial e proporcionando maior segurança das informações o protótipo não permite o *copy and paste*. Todos estes fatores englobam uma estrutura de vários elementos chaves que foram elaborados com o intuito de formar uma arquitetura.

No modelo proposto por [27], um dos fatores de relevância para os autores, é a definição do tipo de distribuição. Conforme o trabalho, os tipos de distribuição devem ser baseados de acordo com suas finalidades, então dois tipos são propostos: PBT (*Payment-Based Type*) e PFT (*Payment-Free Type*). No tipo PBT, um pagamento é solicitado para que o usuário possa ter acesso a informação digital e no tipo PFT, a distribuição pode ocorrer sem a necessidade de um pagamento.

Segundo [45], existem algumas arquiteturas que controlam a disseminação dos conteúdos. Destacando como um de seus pontos principais, [45] sugere em seu modelo uma escala de medição. A escala tem três divisões, sendo elas, pequenas, médias e grandes escalas. Um típico exemplo são as transações *Business to business* classificadas de pequena escala. Os textos e jornais técnicos compreendem a média escala, e a terceira escala é composta por músicas e livros eletrônicos.

O protótipo SUMMER (*Secure Multimedia Retrieval*) [41], procura demonstrar como pode funcionar uma arquitetura DRM, baseando-se em componentes formados em hierarquia (identificação, autenticação etc.). O protótipo define uma arquitetura robusta através da utilização de linguagens como Java e JSP *(Java Server Pages)*. Um *plug-in* também é proposto pela arquitetura e formulado em C++.

Todos os trabalhos correlatos buscam expor fatores que possam contribuir na formação de uma padronização para a tecnologia DRM, sendo assim, uma melhor visão dos estudos relacionados é demonstrada nas próximas seções.

5.1 Protótipo SUMMER

A maioria dos sistemas na "vida real" delegam (comandam) responsabilidades para diferentes autoridades, e o protótipo SUMMER (*Secure Multimedia Retrieval)* aplica esta idéia. Neste modelo uma hierarquia de autoridades emite certificados que são ligados por meios de criptografia, estabelecendo assim uma cadeia de controle: identificação - atributos - direitos, isto permite uma flexibilidade de controle de direitos sobre o conteúdo [41].

Típicos objetivos de segurança como identificação, autorização, autenticação, e controle de acesso podem ser realizados. O estudo realizado para desenvolver o sistema também avaliou algumas plataformas comerciais DRM[11] para a venda de conteúdo digital na web. Um dos resultados demonstrou que algumas indústrias cinematográficas e musicais tais como Sony e Universal, adotaram modelos de negócio on-line, como o modelo *pay-per-view*. Sistemas comerciais são proprietários e incluem componentes chaves proprietários; O SUMMER propõe um sistema aberto e procura demonstrar certa flexibilidade no gerenciamento.

Embora procure demonstrar toda a flexibilidade do sistema, o SUMMER também admite que os componentes para identificação, autenticação e autorização utilizados normalmente quando aplicados ao DRM, criam uma certa limitação. Um exemplo é encontrado nas variedades de permissões oferecidas, neste caso mais flexibilidade é necessária porque ninguém pode prever quais tipos de permissões e direitos que serão

1.1 [11] Tabela demonstrada na seção "Plataformas de Sistemas DRM".

necessários no futuro [41]. Segundo os autores, pode-se criar uma padronização no sistema de controle de acesso, mas quando um novo tipo de permissão é adicionado para o sistema, se faz necessário à associação de todos os sub-objetos e objetos que devem ser revisados e isto acaba criando um problema de gerenciamento.

Na expectativa de diminuir estes problemas, o protótipo introduz um segundo nível de gerenciamento e controle, que tem propósito duplo.O segundo nível refina o primeiro nível de controle e provê facilidades para a distribuição segura do conteúdo. Tudo isto acaba formando o SABDRM= controle de acesso + DRM, ou seja, (*security attribute based digital rights management*). A associação entre estas três identidade de propriedades, de atributos e de direitos representam uma cadeia de controle.

5.1.1 Cenário de aplicação

A figura 3, procura demonstrar o usuário em um cenário de uma organização, Alice é uma "Funcionária" que deseja acessar algum documento em uma base dados, em um sistema de uma organização.

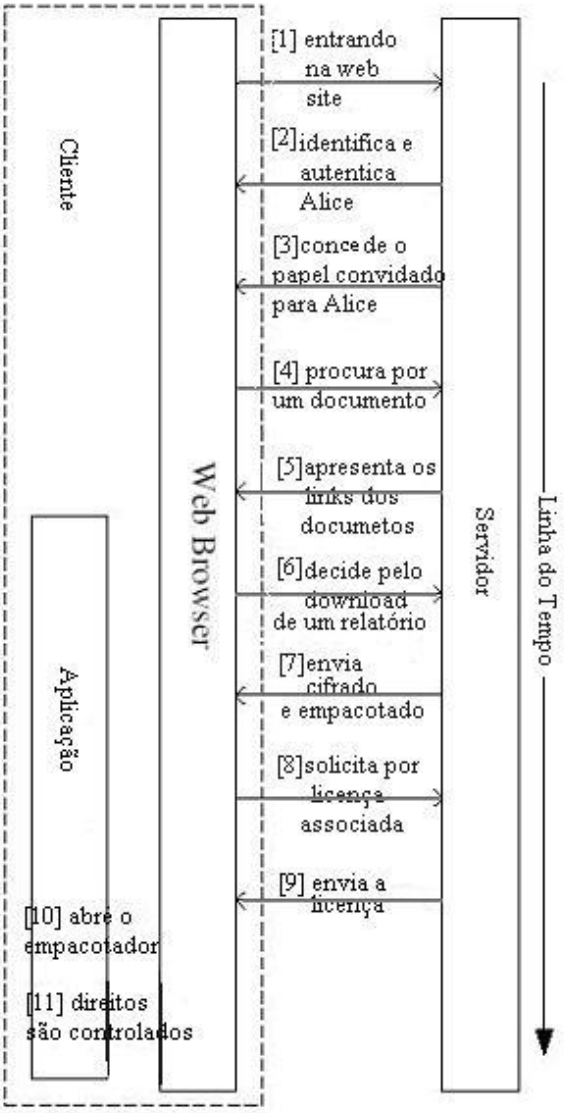


Figura 3.“Usuário em um Sistema” [41].

Os passos referentes à figura 3, estão descritos em ordem numérica como está demonstrado na figura.

1) Alice entra no sistema usando um *Web browser*, depois em um *web site* para o *download* de algum documento de uma organização.

2)O servidor identifica e faz a autenticação, utilizando o certificado de chave pública dela.

3) O servidor concede o papel “Convidado” para ela entrar no sistema.

4) Ela pesquisa pelo documento que deseja acessar, ou com outra categoria de nome, ou ainda com palavras chaves.

5)Com o papel de "Funcionário" o servidor mostra uma lista de documentos (segundo pesquisa) e permite o acesso.

6) Ela decide pelo *download* de um relatório técnico de projeto, de uma organização.

7)O relatório técnico está cifrado, empacotado, e é enviado para Alice.

8)Alice precisa da licença associada "licença do relatório técnico" para acessar a figura digital protegida. Sendo assim ela solicita ao servidor.

9)O servidor recupera os direitos que ela tem segundo "Funcionária" fazendo uma pesquisa em uma base de dados. O servidor embute os direitos e a chave do conteúdo digital na geração da licença, e envia a licença a Alice.

10) Alice tem o relatório técnico protegido e a licença digital associada, ela está agora habilitada a abrir o relatório com a aplicação apropriada.

11)Ela está proibida de imprimir, salvar e transferir o relatório, porque a licença somente permite que ela visualize a figura.

5.1.2 Arquitetura Summer

A figura 4 demonstra uma visão mais completa da arquitetura SUMMER.

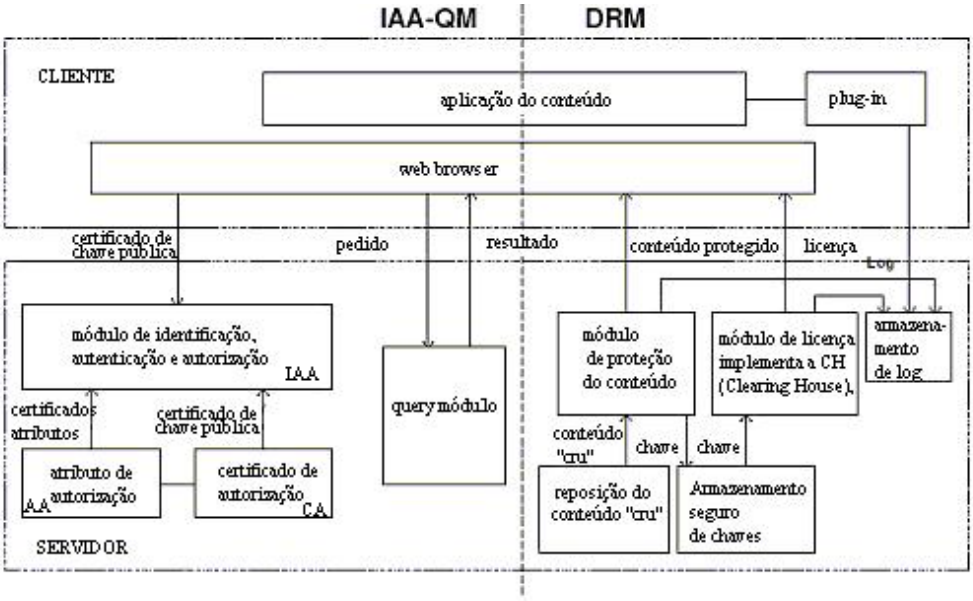


Figura 4."Arquitetura geral protótipo SUMMER" [41].

5.1.2.1 Lado IAA-QM (Identifcation, Authentication and Authorization -Query Module)

O módulo de identificação, autenticação e autorização (IAA), decide a identidade do usuário e estabelece os atributos de segurança para identificação [41]. Então o IAA começa a cadeia de controle de identificação de atributos. Os certificados de atributos e certificados de chave pública, como são gerados e distribuídos pela AA (atributo de autorização), e CA (certificado de autorização) respectivamente, são usados como meios para alcançar IAA.

O *Query* Módulo (QM) estabelece o controle de acesso em um sistema. Ele age como um filtro e monitora o ambiente através de pedidos do cliente e resultados do servidor. O pedido e o resultado são descritos utilizando XML. Uma política de segurança arquiva, e os atributos do cliente são enviados para um ambiente. O resultado exibe uma lista de conteúdo digital acessível segundo o atributo do cliente.

5.1.2.2 Lado DRM

Quanto à parte do DRM (metade direita da Figura 4), ela é composta de quatro componentes, Módulo De Conteúdo, o Módulo De Licença, Aplicação do Conteúdo e o *Plug-in*. À parte do DRM completa a cadeia de controle iniciada pela IAA-QM, para ligar os direitos digitais para identificar atributos. O Módulo de Conteúdo é composto dos seguintes sub-componentes: Proteção do conteúdo, reposição do conteúdo "cru" e armazenamento seguro de chaves. O sub-componente proteção do conteúdo gera, personaliza, e armazena a chave cifrada do conteúdo digital em um modo seguro. Já o segundo sub-componente (reposição do conteúdo), seguramente armazena a decifragem do conteúdo digital. E o seguro armazenamento de chaves, armazena a chave de conteúdo gerada pelo módulo de Proteção.

Já o módulo de licença implementa a "CH" (*Clearing House*), que gera licenças digitais, como encapsulamento de direitos, termos e condições de uso do conteúdo digital. Também recupera a chave de conteúdo digital associada à chave armazenada, codificado por usar a chave pública do cliente embutindo assim, tudo na licença digital.

Os atributos de segurança de um usuário e a identificação do conteúdo digital, são incluídas dentro do modulo de licença, para a geração da mesma. O Módulo De Licença necessita dos atributos de segurança para recuperar uma lista de direitos de acesso, que o usuário possui para o conteúdo e a licença é criada sob demanda e armazenada. A licença digital é assinada usando chave privada do servidor, e os *logs* armazenam os registros de transações. Sendo assim, os registros dos *logs possuem algumas finalidades como*:

- Proteger o conteúdo e o tempo de *download* no lado do servidor;
- O tempo de geração da licença ao lado do servidor;
- Interpretação da licença pelo *plug-in* ao lado do cliente.

O armazenamento de *Logs*:

- Provê uma completa visão de todas as ações que o cliente tem feito sobre o conteúdo digital;
- Pode ser usado em um processo de não repudiação, para exame, e se necessário contabiliza.

Todas as comunicações do *plug-in* (registros do *Plug-in)* são assinadas por usar chave privada de cliente, para impedir que qualquer envio ou recebimento de mensagens sejam negadas; E no lado do cliente, um *Web browser,* é utilizado como uma *interface* para comunicação entre o cliente e o servidor.

5.1.3 Plataformas de Sistemas DRM

Os estudos realizados no desenvolvimento do protótipo SUMMER geraram uma comparação entre plataformas conforme é demonstrado na tabela 1:

DRM	**APLICAÇÃO**	**CARACTERÍSTICAS**	**CONTEÚDO**
Microsoft	Windows Media Player	*#As licenças são descritas usando XrML.* *#fim a fim, proteção persistente, licenças e chaves procuram arquivos media.* *#Caminho de áudio Seguro para prevenir um programa não autorizado de fazer alguma captura.*	Áudio, e vídeo
IBM	EMMS player SDK	*#Fornece uma proteção resistente, ambiente para acessar e gerenciar o áudio.* *#Utiliza recipientes seguros para contrariar o uso não autorizado da música digital protegida.* *#Utiliza criptografia para proteger as chaves.* *#Produz logs para todas as transações.*	Áudio
Content Guard	SDK	*#Produz os rótulos de direitos durante preparação de conteúdo. O rótulo de direito é utilizado para gerar a licença quando a licença é solicitada.* *#Produz relatórios e auditoria da transação dos logs*	Alguns tipos de formato de conteúdo digital
Inter Trust	Toolkits	*#Atualiza o sistema automaticamente para instalar correções.* *#Fornece um DRM somado em chip para a segurança da arquitetura do microprocessador.* *#Suporta múltiplos padrões de criptografia.*	Alguns tipos de formato de conteúdo digital
SealedMedia	Unsealer (*browser plugin*)	*# Divide em categorias o conteúdo digital, e uma licença digital.* *#Implementa um clock de confiança na aplicação, sincroniza com o servidor de licença.*	HTML, GIF, JPEG, PDF, MP3, video.
SUMMER	*Plug-in* para Adobe Acrobat	*#Produz a proteção do empacotamento do conteúdo digital e gera a licença sob demanda.* *#Personaliza a chave do conteúdo para um usuário.*	No momento somente PDF.

Tabela 1.“Breve comparação de plataformas DRM, com o protótipo Summer” [41].

Os desenvolvedores do Protótipo SUMMER acreditam que seguindo e aperfeiçoando a arquitetura proposta, os seus objetivos de participar do mercado do DRM possa ser alcançado; abrindo assim, um comércio digital seguro onde os usuários podem comprar e vender seus conteúdos digitais sem infringir o *copyright*.

5.2 Arquitetura de Segurança para Controlar a Disseminação da Informação Digital

Atualmente várias aplicações para soluções de segurança que possam controlar a disseminação da informação digital são desenvolvidas utilizando criptografia e *watermarking*. Estas disseminações de soluções de controle projetam-se para diferentes modelos de negócios eletrônicos. Dessa forma para formular uma solução segura se faz necessário identificar os tipos de distribuição que são utilizadas pelos modelos de negócios.

Segundo [27], existem dois tipos de distribuição de conteúdos, estes são baseados de acordo com suas finalidades. *Payment-Based Type* (PBT), compreende o primeiro tipo, no qual um pagamento é requisitado se adquirir a informação digital. Já no segundo tipo, *Payment-Free Type* (PFT), a disseminação da informação digital não requer o pagamento, mas deve ser controlada com o objetivo de satisfazer a confidencialidade, ou outras exigências da segurança.

Os estudos realizados por [27], são focados em *Payment-Free Type* (PFT). As características da informação digital do ambiente de PFT diferem significativamente das características da informação digital do ambiente de PBT. No (PBT), um pouco de vazão da informação é aceitável e desejado [44], mesmo quando isto não pode ser aceitável para o ambiente de PFT, já que o objetivo do PBT é vender.

O número de cópias legítimas de um único artigo digital em PBT é tipicamente maior que o de cópias de PFT, pois no geral o objetivo no ambiente de PBT é distribuir tantas cópias quantas possível, e extrair o pagamento para cada uma delas.

No ambiente de PFT é a própria distribuição que necessita ser limitada, conseqüentemente, as soluções e pesquisas para finalidades baseadas em pagamento não podem ser diretamente aplicáveis ao ambiente de PFT, como exemplo estão as transações de B2B. Em PBT as rupturas da segurança de recursos digitais resultam diretamente na perda financeira (B2B).

Hoje os esforços para proteger a informação digital de distribuição não autorizada, são originados pela grande maioria dos fornecedores digitais insatisfeitos. Entretanto, nenhum estudo sistemático foi feito, controlando a disseminação da informação digital. Nos estudos realizados por [27], destacam-se três grandes componentes em arquiteturas de segurança DRM, cada um com suas vantagens e desvantagens, resulta em diferentes arquiteturas. Os três componentes presentes em arquiteturas DRM são:

- *Virtual machine* / máquina virtual (VM);
- *Control set* / conjunto de controle (CS) e
- *Distribution style* / estilo de distribuição.

A máquina virtual é um *software* que é localizada no lado do cliente, para controlar e administrar o acesso e uso da informação digital. Um exemplo deste caso é a *Adobe Acrobat Reader* com a compra do *plug-in web*. A existência de uma máquina virtual no lado do cliente é uma maneira de influenciar a arquitetura, isto fornece a base e controle de tecnologias, também implica na necessidade de softwares e hardwares especializados ao lado cliente.

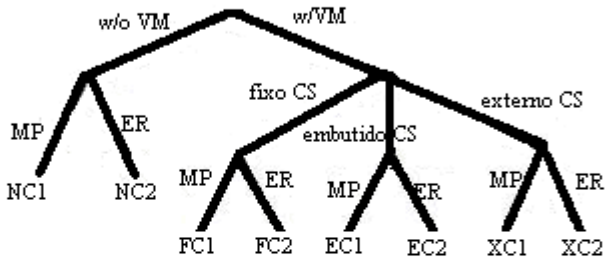
Quanto ao conjunto de controle, pode-se dizer que é uma lista de direitos de acesso e usa regras que são aplicadas pela (MV), as quais controlam ambientes de acesso e usam informação digital. Os conjuntos de controle são determinados pelos estilos de distribuição do conteúdo. A interpretação da figura 5, procurou manter as siglas originais da obra, interpretando somente seus significados. A sigla (MP) “Envio de mensagem” e a sigla (ER) “repositório externo” são dois estilos de distribuição possíveis. Em (MP), a informação digital é enviada para cada recipiente (cliente), enquanto em (ER), cada cliente obtém a informação digital a partir de um servidor em uma rede. A classificação da arquitetura é baseada nos três fatores já descritos: máquina virtual (VM); conjunto de controle (CS) e estilo de distribuição. Estes também são brevemente ilustrados na figura 5.

VM: Máquina Virtual

MP: Mensagem Enviada

ER: Repositório Externo

CS: Conjunto de Controle



NC1: sem controle w/MP

NC2: sem controle w/ER

FC1: controle fixo w/MP

FC2: controle fixo w/ER

EC1: controle embutido w/MP

EC2: controle embutido w/ER

XC1: controle externo w/MP

XC2: controle externo w/ER

Figura 5.“CLASSIFICAÇÃO DA ARQUITETURA” [27].

Na figura 5, a sigla (NC) “sem controle”, significa a falta de uma máquina virtual, e quanto a sigla (FC) “Controle fixo”, é a forma onde só o controle permanece fixo na máquina virtual.

As siglas (EC) e (XC), controle embutido e controle externo, são meios de controle que podem variar, sendo assim, eles podem coexistir como controles fixos em uma máquina virtual. A figura 6, procura demonstrar melhor um exemplo de funcionamento da taxonomia proposta na figura 5.

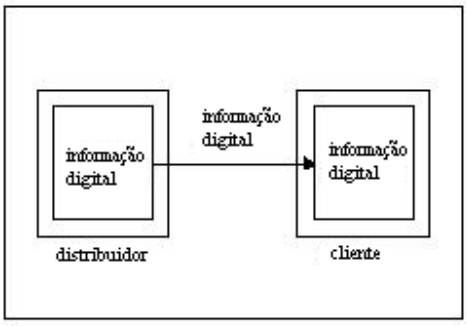


Figura 6 "Sem Controle com Mensagem Enviada (NC1)" [27].

No exemplo demonstrado através da figura 7, o distribuidor envia uma cópia do conteúdo digital para cada cliente, e cada cliente armazena a cópia da informação digital em um local de armazenamento. Depois de distribuído não existe meios de controlar a informação distribuída, e para acessar a informação vinda de um sistema múltiplo, o cliente precisa transportar a informação.

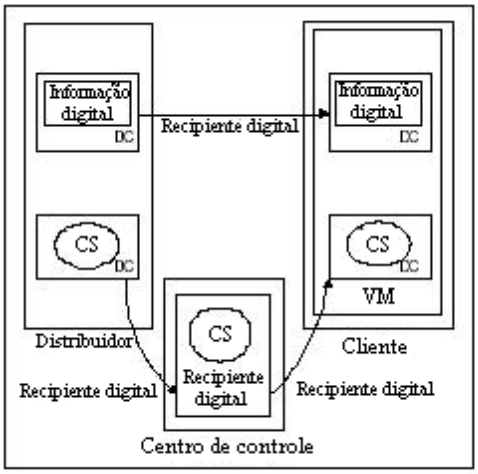


Figura 7 "Controle Externo com Mensagem Enviada (XC1)" [27].

Ainda procurando esclarecer a arquitetura apresentada na figura 5, o exemplo oferecido pela figura 7, demonstra que o conjunto de controle pode ser encapsulado independente do conteúdo digital, gerando duas opções possíveis: a primeira opção é conectar a rede sempre que requerer o conteúdo. Já a segunda hipótese, é que uma conexão da rede seja requerida de tempos em tempos.

Este estudo realizado por [27], procura demonstrar fatores importantes no desenvolvimento de uma arquitetura para a distribuição digital de conteúdos, expondo métodos e soluções que visam o crescimento da tecnologia DRM.

5.3 Uma estrutura de Framework para Controle de Uso e Gerenciamento Digital de Direitos.

Conforme descrito na sessão anterior, DRM pode ser usado tanto para *Payment-Based Type* (PBT) como *Payment-Free Type* (PFT), sendo este um dos motivos em que o *"UCON - Usage Control"* (controle de uso), torna-se um método que busca abranger ambos os casos. Para os (PBT), a principal motivação é a geração e proteção da renda derivada do conteúdo digital, já para os (PFT), a motivação é o interesse pela confidencialidade e privacidade [45].

UCON é uma estrutura de engenharia que inclui todos aspectos de políticas, modelos, arquiteturas, e mecanismos para controlar e seguir o acesso do uso de objetos digitais [45]. UCON unifica o controle de acesso, a gerência de confiança, e gerenciamento digital de direitos e vai além em suas definições e áreas de interesse. De acordo com [45], os recentes assuntos gerados por P2P *"peer-to peer"* arquivo compartilhado, é um exemplo do desafio que o controle enfrenta.

O conceito principal de DRM é originalmente baseado no paradigma de "superdistribuição" onde a informação eletrônica está livremente disponível, mas o acesso para a informação é controlado [44]. Devido a vantagem comercial que as soluções do DRM podem fornecer, o esforço maior em estudar e desenvolver soluções DRM têm sido dirigidos pelo setor comercial. Sendo assim, utiliza-se o controle de uso para estudar estas soluções.

Na perspectiva de segurança de informação, o "*UCON"* (controle de uso) se torna tão vital quanto os três objetivos famosos de confidencialidade, integridade e disponibilidade, assim deveria ser considerado como um quarto objetivo adicional [45].

O controle de uso "*UCON"* tenta solucionar problemas que não são considerados nas resoluções típicas de DRM, entre os problemas destaca-se a questão da privacidade.

Então, controles de uso com funções de privacidade devem ser incluídos nestes sistemas, por exemplo: A lei "*healthcare"* (cuidados com a saúde) do Reino Unido, designa que os sistemas de *"healthcare"* devem permitir aos pacientes, decisões como o que pode se ter acesso em seu histórico ou até mesmo saber quem acessou suas informações.

O controle de uso também se preocupa com soluções que promovem as transações B2C (*business to consumer*) e B2B (*business to business*); para permitir transações B2B seria necessário gerar maneiras que possam controlar o uso da informação digital entre as organizações. Estas são algumas das muitas áreas que podem ser consideradas em sistemas de UCON. Embora as soluções DRM sejam bem sucedidas, não há nenhuma que possa ser considerada uma referência padrão na comunidade [45].

Todos estes motivos levam a análise e proposta de sistemas UCON.

5.3.1 O OM-AM Framework

O OM-AM *framework* proposto no trabalho de [45], é a primeira e recente proposta de engenharia de "*framework"* que permite o desenvolvimento de novos modelos de controle de acesso como o DRM.

OM-AM apresenta no seu raciocínio, o objetivo, o modelo, a arquitetura e o mecanismo, respectivamente. As camadas objetivo e modelo articulam o que os objetivos da segurança são e o que deve ser conseguido. Quanto à arquitetura e o mecanismo, estes descreve como conseguir estes objetivos e exigências. A Figura 8 apresenta um diagrama da estrutura de OM-AM.

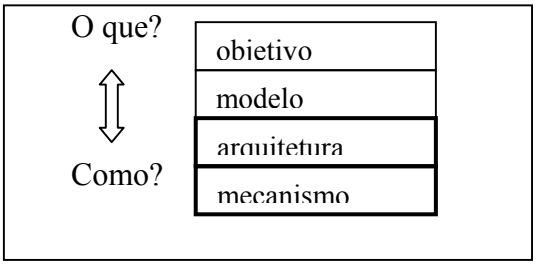


Figura 8 "OM-AM Framework" [45].

No mundo real, os objetivos para soluções de "*UCON"* podem variar, cada solução tem um caso diferente a alcançar, os detalhes de suas exigências podem alterar de caso para

caso. Os fatores devem ser considerados parte dos objetivos [45]. Estes incluem escalas de "*PBT"* ou *"PFT"*, em ambientes de disseminação, prevenção e detecção. Além destes fatores, pode haver muitos outros que influenciam aproximações individuais das soluções. Para compreender melhor, a tabela 2, mostra algumas características dos fatores "*PBT"* e "*PFT"*.

CARACTERÍSTICAS	**PBT**	**PFT**
Vazamento	Aceitável ou mesmo desejável.	Não aceitável.
Número de cópias por item	Alto volume.	Baixo volume.
Propósito	Aumento de renda.	Disseminação limitada.
Acesso	Através de pagamento.	Controle de Acesso obrigatório (MAC), Controle de acesso dicionário (DAC).

Tabela 2 "Características de PBT e PFT" [45].

Estes fatores podem influenciar todas ou algumas camadas do modelo, arquitetura ou mecanismo. A consideração cuidadosa destes fatores fornecerá uma compreensão melhor dos problemas de sistema de controles de acesso, e conseqüentemente limites e exigências mais exatos da solução. De acordo com [45], as escalas das disseminações são baseadas nos volumes da disseminação do objeto da informação digital, e são divididas em 3 escalas, pequena, média, e grande, como demonstrado na figura 9.

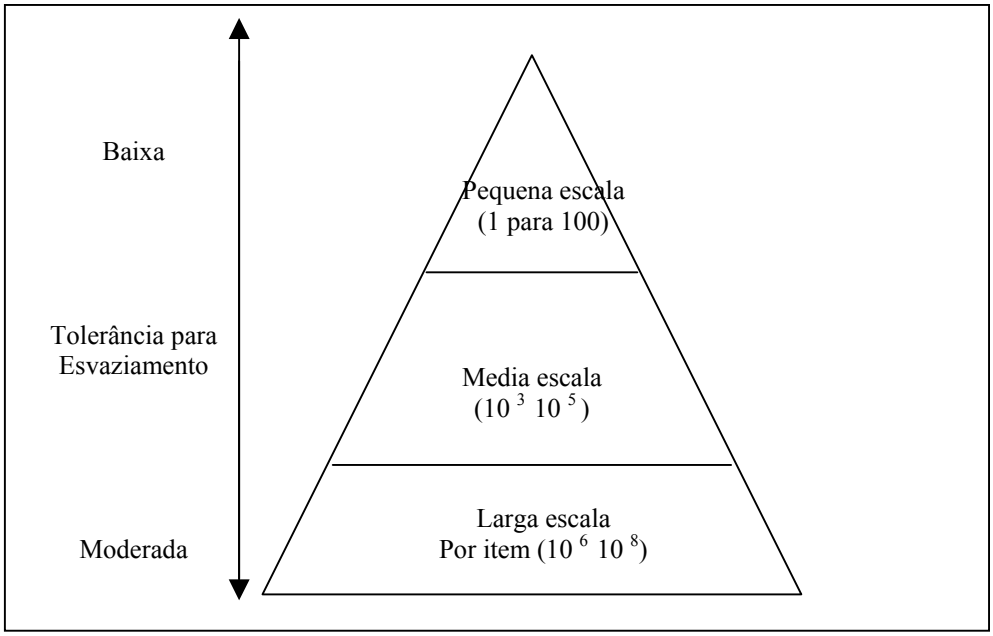


Figura 9 "DISSEMINAÇÃO DA ESCALA" [45].

Na disseminação *small-scale*, cada artigo da informação digital é distribuído aproximadamente de um para cem receptores. As transações do B2B são exemplos típicos da disseminação em pequena escala. Na disseminação *medium-scale*, cada artigo da informação digital é distribuído de 10^3 a 10^5 receptores; os textos ou os jornais técnicos são os objetos desta escala. Na disseminação em *large-scale*, cada artigo da informação digital é distribuído aproximadamente de 10^6 a 10^8 receptores; os arquivos de música, tais como *MP'3s*, ou livros eletrônicos (*e-books*) são alguns dos exemplos. Os números dados não são valores absolutos, mas indicam uma escala geral para o tamanho da distribuição [45].

5.3.2 O Modelo UCON

Sistemas de UCON são formados por diversos componentes chaves. Segundo [45], na camada do modelo de controle de uso, não é considerado como executar sistemas da solução do UCON usando estes componentes chaves; isto é, deixando para as camadas de arquitetura e mecanismo.

O modelo de controle de uso é dividido em dois lados: o lado do consumidor e outro do fornecedor, sendo que cada lado consiste nos seguintes seis componentes principais: sujeito, objeto, direitos, condição, obrigação, e da autorização onde o componente objeto é comum a ambos os lados como é representado pela figura 10.

Dividindo o modelo UCON entre o lado do consumidor e o lado do fornecedor pode-se entender melhor cada componente e os relacionamentos entre eles. Seus direitos (direitos do consumidor e direitos do fornecedor) são completamente diferentes. Conforme [45], esta não é uma descrição completa de modelos de UCON, e sim um estudo preliminar no assunto que pretende fornecer idéias gerais. Os estudos em um modelo mais detalhado requerem melhores esclarecimentos e refinamentos.

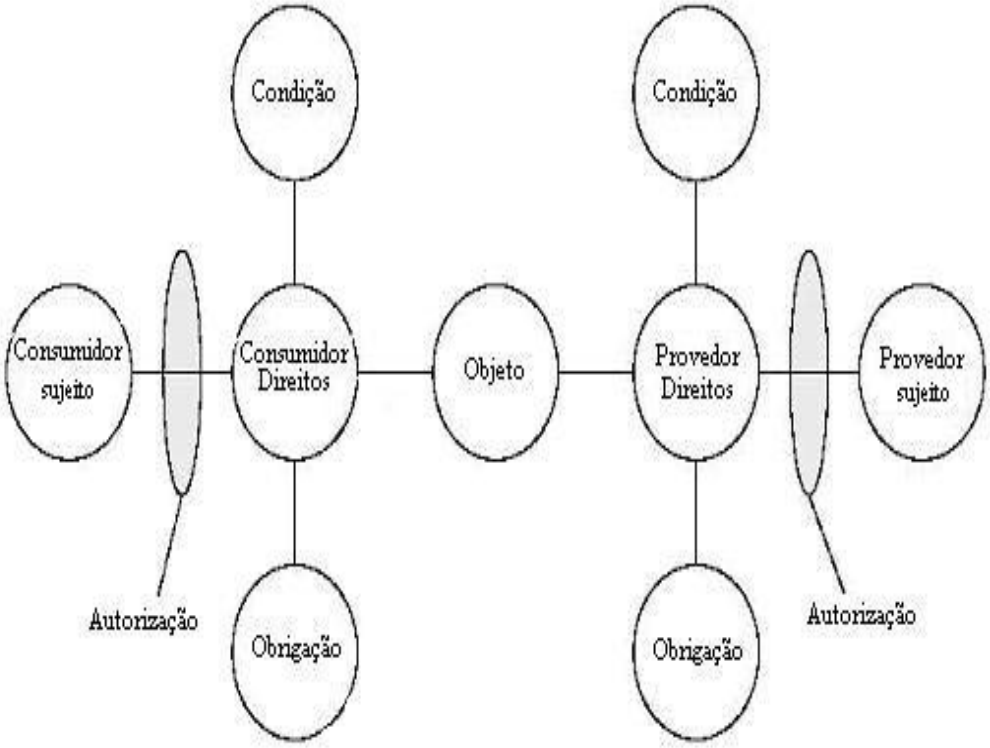


Figura 10 "MODELO E COMPONENTES DE UCON" [45].

A tabela 3, demonstra alguns modelos de componentes e exemplos, esclarecendo melhor o modelo de UCON apresentado na figura 10.

COMPONENTES	EXEMPLOS
SUJEITO	Publicador, paciente, leitor, distribuidor, medico, autor, músico, etc.
OBJETO	Documento digital, arquivo áudio, arquivo vídeo, arquivo de jogo, etc.
DIREITOS	Direitos de consumidor: ver/jogar, imprime, editar, copiar, etc. Provedores de direitos: Coleta taxas de uso e usa informações de log, escolhe as regras que usa.
OBRIGAÇÃO	• Consumidor tem que aceitar acordo de medidas de pagamento para o uso de certa informação digital. • Consumidor deveria informar uso da informação de log para o provedor de sujeitos. • Consumidor tem que concordar com o pagamento (que deduz a quantidade de carga de seu cliente) com o acesso a um objeto da informação digital. • Consumidor tem que concordar com o relatório da informação local da configuração de sistema. • Provedor tem informar consumidor que registro de uso deve ser informado a ele. • Provedor tem que informar o consumidor de taxas de uso. • Provedor tem que concordar na parte de distribuidor de lucro.
CONDIÇÃO	• Partes Acessíveis baseadas em logs de uso. • Período do tempo Acessível. • Localização Acessível. • Permitido nome de impressora.
REGRAS DE AUTORIZAÇÃO	• Rótulo de Segurança. • Certificado de Papel. • Atribui certificado. • Pagamento.

Tabela 3 "Modelos Componentes UCON e Exemplos" [45].

A arquitetura UCON segue o mesmo modelo citado na seção "Arquitetura de Segurança para Controlar a Disseminação da Informação Digital", onde esta destaca três fatores que formam a arquitetura: *Virtual machine* / máquina virtual (VM); *Control set* / conjunto de controle (CS) e *Distribution style* / estilo de distribuição.

5.4 Conclusão do Capítulo e Considerações sobre os Trabalhos Relacionados

Neste capítulo foram demonstrados os trabalhos [41, 27,45], e realizou-se uma breve explanação sobre o protótipo desenvolvido neste trabalho. Todos os trabalhos descritos buscam contribuir para a formação de um padrão DRM.

O protótipo SUMMER trabalha com componentes formados por uma hierarquia de autoridades que emite certificados, estabelecendo assim uma cadeia de controle: identificação - atributos - direitos, isto permite uma flexibilidade de controle de direitos sobre o conteúdo [41]. Esta flexibilidade pode ser alcançada a partir do momento em que se conhece o usuário e estabelece os direitos que o mesmo possui. O protótipo trabalha apenas com arquivos em formato PDF, e que podem ser lidos por um *plug-in* no Adobe Acrobat (www.adobe.com). Quanto a distribuição do conteúdo, ele pode somente ser disseminado de forma completa, ou seja, não pode ser distribuído em partes ou em "fatias".

Na arquitetura do protótipo SUMMER os direitos são separados dos conteúdos, e portanto pode ser classificado como uma arquitetura do tipo XCII da taxonomia de [27]. Baseando-se em [27], outras formas de arquiteturas podem contribuir na evolução do protótipo SUMMER, as quais foram descritas no capítulo quatro.

O estudo realizado por [27], define uma taxonomia para arquiteturas DRM, levantando formas de organizar e armazenar conteúdos e direitos. Esse trabalho não contribui com experimentos práticos, mas tenta direcionar essa nova área de pesquisa na segurança de sistemas.

As pesquisas [27,45], estipulam dois tipos de distribuição de conteúdos, (PBT) e (PFT). Segundo [27], suas pesquisas são mais focadas para o tipo PFT, pois o número de cópias legítimas de um único artigo digital em PBT - é tipicamente maior que o de cópias de PFT. Isto ocorre devido a maior distribuição de documentos do tipo PFT, ocasionando maiores oportunidades e facilidades para modificações de um documento.

Atualmente muitas soluções são baseadas em distribuição PBT, principalmente em grandes modelos de negócios, já que de forma geral o objetivo no ambiente de PBT é distribuir tantas cópias quantas possível, e extrair o pagamento para cada uma delas. Este fator acaba gerando um mercado de soluções, proporcionando uma enorme área de estudos e contribuições para a tecnologia DRM.

A utilização de uma máquina virtual no lado do cliente é uma das sugestões de [27, 45], que pode ser aproveitada para pesquisas mais aprofundadas, proporcionando oportunidades de estudos referentes a segurança no desenvolvimento de um *plug-in* ou *software* no lado do cliente. Pesquisas sobre como e onde os direitos devem ser armazenados, e também como ocorre o funcionamento de um *plug-in* no lado do cliente, justificam algumas destas oportunidades que podem ser estudadas de forma mais aprofundada. [45] ainda propõe que os modelos de controle de uso solucionem questões de privacidade. Todas as propostas estudadas para o desenvolvimento de uma estrutura DRM fornecem pontos de pesquisas como posição e armazenamento dos direitos, controle de acesso, software no lado do cliente entre outras, que ainda podem ser aprofundados e complementados através de novas idéias e recomendações. A tecnologia DRM ainda não possui um padrão, questão esta que serve de motivação para novos estudos.

6 Ferramentas para Implementação

Este capítulo descreve as tecnologias usadas para implementar e validar a

arquitetura e o *plug-in* para controle da disseminação de conteúdo digital, propostos no capítulo sete.

6.1 JAVA

Conforme [69], Java é ao mesmo tempo um ambiente e uma linguagem de programação orientada a objetos desenvolvida pela *Sun Microsystems*, capaz de criar tanto aplicativos completos e independentes, como aplicativos para páginas *Web*, sendo assim, é construída de tal forma a possibilitar que seus programas, depois de compilados, possam rodar em qualquer plataforma. Além disso, caracteriza-se por ser muito parecida com C++, eliminando as propriedades consideradas complexas, como aritmética de ponteiros.

6.1.1 Applets x Aplicativos

Programas escritos em Java podem ser *Applets* ou Aplicativos. Aplicativos são programas que necessitam de um interpretador instalado na máquina [70]. Enquanto que *Applets* são programas carregados juntamente com páginas HTML, e o interpretador está inserido no próprio *browser,* não necessitando de instalação, basta apenas que o *browser* usado ofereça suporte a Java.

6.1.2 Software Development Kit - SDK

O SDK é um kit de desenvolvimento Java fornecido livremente pela Sun. Constitui um conjunto de programas que engloba compilador, interpretador e utilitários. A primeira versão deste *Kit* foi a 1.0 e atualmente encontra-se em 1.4.2, cada uma delas com atualizações. De acordo com [73], os principais componentes do *kit* de desenvolvimento são:

- javac (compilador);
- java (interpretador);

- appletviewer (visualizador de applets);
- javadoc (gerador de documentação);
- jar (programa de compactação).

A utilização do SDK é feita da seguinte forma: primeiro escreve-se o programa fonte em Java, utilizando qualquer editor de texto. A seguir, o programa deve ser compilado utilizando o compilador **javac.**

A compilação gera o arquivo em código binário (*bytecodes*), com extensão.*class*. Uma vez compilado, basta interpretar o arquivo compilado; Se for uma aplicação, utiliza-se o interpretador **java.**

Sendo um *applet*, deve-se construir uma página HTML para abrigar o *applet* e carregá-lo através de um *browser* ou do ***appletviewer.***

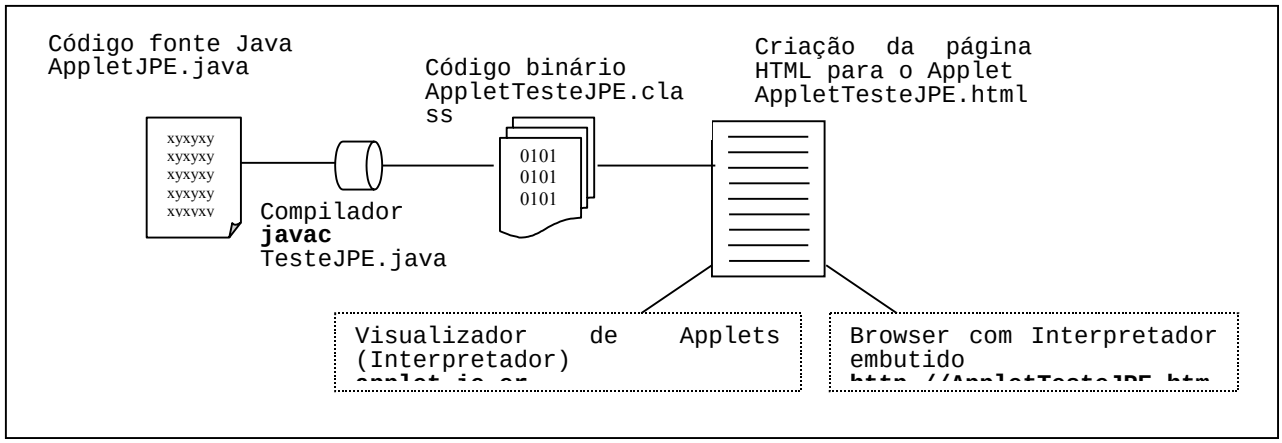


Figura 11 "APPLET"

6.1.3 Características da linguagem

Java também é conhecida como uma Linguagem simples e de fácil utilização, possui sintaxe muito parecida com C++, considerada uma das linguagens mais difundidas atualmente.

Um programa desenvolvido em Java necessita ser compilado, gerando um arquivo de *bytecodes*. Para executá-lo é necessário então, que um interpretador leia o código gerado em *bytecodes* e repasse as instruções ao processador da máquina específica. Esse

interpretador é conhecido como JVM (*Java Virtual Machine*). Segundo [75], os *bytecodes* são conjuntos de instruções, parecidas com código de máquina, é um formato próprio do Java para a representação das instruções no código compilado.

A máquina virtual (JVM) evita que os programas causem danos ao computador no qual os programas são executados. Faz com que os programas sejam descarregados rapidamente e executa-os para que sejam independentes do sistema operacional, fornecendo assim grandes funcionalidades para trabalhar em rede, através das APIs [75].

Programas Java são ligados em tempo de execução. Os *bytecodes* gerados durante a compilação só serão integrados na execução. Se alguma alteração ocorrer na classe que define o objeto, somente o arquivo da classe com a alteração, necessita ser compilado.

Um código Java pode ser executado em qualquer arquitetura de hardware e sistema operacional, sem precisar ser recompilado. Um programa Java pode ser executado em qualquer plataforma que possua um interpretador Java (ambiente de execução) [70].

O Java fornece uma série de mecanismos e módulos de criptografia para garantir a segurança das aplicações. De acordo com [72], um programa Java não tem contato com o computador real; ele conhece apenas a máquina virtual, sendo assim a máquina virtual decide o que pode ou não ser feito. Um programa nunca acessa dispositivos de entrada e saída, sistema de arquivos, memória, ao invés disso, ele requisita a JVM que realiza o acesso.

6.1.4 JCE – Criptografia

O Java *Cryptography Extension* – JCE, é um conjunto de pacotes que provêm um *framework* e implementações para criptografia, geração e autenticação de chaves, bem como algoritmos de Código de Autenticação de Mensagem – MAC. O Suporte para criptografia inclui cifras simétricas, assimétricas, de bloco e fluxo (*stream*). O JCE 1.2 foi criado para estender as APIs Java *Cryptography Architecture* - JCA disponíveis na plataforma Java II [77].

JCE se baseia nos mesmos princípios de projeto encontrados em outros lugares do *framework* da Arquitetura de Criptografia Java, utilizado por todos os componentes de

segurança relativos a criptografia da plataforma Java II: independência da implementação e, sempre que possível, independência do algoritmo [77]. Ele usa a mesma arquitetura "provedor", que usa a noção de Provedor de Serviço Criptográfico, ou "provedor" como abreviação. Este termo se refere ao pacote (ou um conjunto de pacotes) que fornece uma implementação concreta de um subconjunto dos aspectos criptográficos da API de segurança Java.

JCE estende a lista de serviços criptográficos da qual um provedor pode fornecer implementações, por exemplo, conter uma implementação de um ou mais algoritmos de assinatura digital e um ou mais algoritmos criptográficos [72].

Um programa desejando usar funcionalidade criptográfica pode simplesmente solicitar um tipo particular de objeto (tal como um objeto criptográfico) implementando um algoritmo particular como DES – *Data Encryption Standard*, e obter uma implementação de um dos provedores instalados. Se uma implementação de um provedor particular é desejada, o programa pode solicitar esse provedor pelo nome, junto com o algoritmo desejado.

6.2 Base de dados MySql e Acesso a JDBC - *Java Database Connectivity*

Há pouco tempo atrás, para adicionar, acessar ou processar uma coleção de dados estruturados, sejam eles uma simples lista de compras a uma galeria de imagens ou até mesmo uma grande quantidade de informação de uma rede coorporativa era considerada uma tarefa árdua para os profissionais de TI.

Buscando facilitar estas operações surgiram os SGBD ou sistemas gerenciadores de banco de dados. Atualmente existem vários SGBD com esta finalidade, entre eles destaca-se o MySQL (*Structured Query Language*) que é um sistema gerenciador de bancos de dados relacional e também é um *software Open Source*, o que garante a sua licença para qualquer pessoa, podendo então usufruir de diferentes formas ou até efetuar modificações.

MySQL foi desenvolvido originalmente para trabalhar com diversas aplicações de maneira muito mais rápida que as soluções existentes, sendo assim, tem sido usado em ambientes de produção de alta demanda por diversos anos de forma bem sucedida [78]. Apesar de estar em constante desenvolvimento, o MySQL hoje oferece um rico e

proveitoso conjunto de funções. A conectividade e a velocidade fazem com que o MySQL seja altamente adaptável para acessar bancos de dados na Internet. Ele é um sistema cliente/servidor que consiste de um servidor SQL multi-tarefa que suporta acessos diferentes, vários programas clientes e diferentes bibliotecas, ferramentas administrativas e diversas *interfaces* de programação.

Quanto as suas funções SQL, são implementadas através de uma biblioteca de classes altamente otimizada gerando maior velocidade no acesso aos dados, geralmente não há nenhuma locação de memória depois da inicialização da pesquisa. Um sistema de privilégios e senhas que é muito flexível, seguro e permite verificação baseada em estações / máquinas, as senhas são seguras porque todo tráfego de senhas são cifradas quando é feita a conexão com o servidor [67]. Existe também as tabelas *hash*, que são usadas como tabelas temporárias. Existem diversos produtos de banco de dados disponíveis no mercado sendo que cada um trabalha com uma linguagem diferenciada.

A API do Java, o JDBC, permite compartilhar uma única linguagem entre as diversas aplicações, além disso, o JDBC - Java *Database Connectivity* - provê um conjunto de *interfaces* com o objetivo de criar um ponto em comum entre as aplicações e os mecanismos de acesso a um banco de dados [65].

Assim, juntamente com grandes líderes da área de banco de dados, a *JavaSoft* desenvolveu uma API simples para o acesso a base de dados - JDBC. Baseado neste processo foi criado algumas metas de projeto tais como:

- JDBC deve ser uma API ao nível de SQL
- JDBC deve absorver as experiências em outras APIs de bases de dados.
- JDBC deve ser simples.

Uma API ao nível do SQL permite construir sentenças SQL e colocá-las dentro das chamadas da API Java [76]. Os resultados das bases de dados são retornados através de variáveis do Java e problemas com acessos são recebidos pelas exceções. Devido aos problemas surgidos com a proliferação dos acessos as APIs dos bancos de dados proprietários, a idéia do acesso ao BD universal não é uma solução nova. De fato, a *JavaSoft* aproveitou todos os aspectos de uma API, a ODBC (*Open DataBase Connectivity*). O ODBC foi desenvolvido com o intuito de criar um padrão de acesso às

bases de dados no ambiente Windows [76]. Embora a indústria tenha aceito o ODBC como um primeiro recurso, o mesmo não se comporta perfeito com o Java. Isso ocorre devido ao fato do ODBC ser uma API desenvolvida em C, e deter uma complexa estrutura interna. Adicionando ao ODBC, o JDBC é fortemente influenciado pelas APIs existentes nos BD tais como X/Open SQL *Call Level Interface*. Assim, a *JavaSoft* se utilizou deste recurso e construiu uma simples API com o intuito de ser aceito pelas empresas de BD.

6.2.1 A Estrutura do JDBC

O JDBC realiza as suas tarefas implementando um conjunto de *Interfaces*, cada conjunto pode ser desenvolvido por um fabricante distinto, sendo que o conjunto de classes que implementa estas *interfaces* são chamadas de *Driver* do JDBC [76]. No desenvolvimento de uma aplicação, não é necessário se preocupar com a construção destas classes, mas somente com a sua utilização e implementação do código que será utilizado.

A aplicação que estiver sendo desenvolvida deve estar desprovida de detalhes contendo, estritamente, a implementação do *Driver* para esta base de dados. Assim, uma aplicação utiliza o JDBC como uma *interface* por onde trafegam todas as requisições feitas ao Banco.

6.2.2 Conexão com o Banco de Dados

Utilizando o endereço da base de dados, um identificador do usuário e uma senha, a aplicação requisita da classe *DriverManager* uma implementação da *java.sql.Connection*. Diante disso, o *DriverManager* realizará uma pesquisa buscando uma conexão de acordo com os dados fornecidos na url. Caso não encontre nenhuma ocorrência do mesmo, será gerada uma exceção na aplicação.

Uma vez que o *Driver* reconheça a URL, ele cria uma conexão com o Banco de Dados utilizando o UserID e o Passwd. Logo em seguida o gerenciador de *driver* envia o objeto *Connection*. Assim, para realizar a conexão, o JDBC utiliza-se de uma classe (java.sql.DriverManager) e duas *interfaces* (java.sql.Driver) e (java.sql.Connection).

- *java.sql.Driver*

Esta *interface* é responsável por responder as requisições dos gerenciadores de *driver* e fornece informações sobre as implementações em questão.

- *Java.sql.DriverManager*

A principal funcionalidade desta classe é manter uma lista de implementações de *Driver* e apresenta. À aplicação um que corresponda ao requisitado através do parâmetro URL [76]. O *DriverManager* contém um método para registrar *Driver* e outra para remover o registro que são respectivamente: *registerDriver*() e *deregisterDriver*().

6.2.3 Acesso à Base de Dados

Uma vez inicializada a conexão através do objeto *Connection* é criada uma linha direta com a Base de Dados onde pode-se manipular as funções do SQL presentes na DML como alteração, ou simplesmente consultas [67]. Assim, a utilização do objeto *Connection* permite gerar implementações da classe *java.sql.Statement* na mesma transação. Após a utilização das Sentenças do SQL é necessário realizar um *commit* (confirmação) ou *rollback* (cancelamento) dos objetos associados na classe *Connection* [76].

Como citado anteriormente, o acesso a base de dados se inicializa com a conexão ao BD através dos objetos da classe *Connection*. Este objeto tem como objetivo armazenar implementações da classe java.sql.Statement em uma mesma transação. É importante se distinguir entre o tipo de sentença SQL que se deseja utilizar, visto que o método de enviar consultas (*query*) difere do envio de atualizações(*update, insert, delete*) na base de dados [67]. A principal diferença ocorre, pois o método da consulta retorna uma instância da classe java.sql.*ResultSet* enquanto que a atualização retorna um número inteiro. O ResultSet permite que se manipule o resultado de uma consulta (*Query*).

- java.sql.Statement

O método *executeQuery()* tem como parâmetro de entrada uma *string*, onde será colocada a sentença SQL, e retorna um objeto ResultSet. As sentenças de atualizações são executadas utilizando o método *executeUpdate()*. Este método retorna um número inteiro se referenciando a quantidade de registros que foram alterados de acordo com esta sentença [67].

Além disso, a classe *Statement* fornece o método E*xecute()* para situações que não se tenha conhecimento do tipo de sentença, se é uma consulta ou uma atualização. Se a

sentença retornar um registro do banco, o método retorna *True,* caso contrário retorna *False*. A aplicação pode utilizar o método getResultSet() para obter o registro retornado.

- Java.sql.ResultSet

Um *ResultSet* é uma linha ou conjunto de dados resultante de uma Consulta (*Query*). A classe permite manipular os resultados de acordo com as colunas da base.

Há ainda o método n*ext()* que permite navegar pelos registros de um *ResultSet*. Se o método *next()* retornar *TRUE* significa que há outra linha na seqüência, e se retornar *FALSE* significa que não falta nenhum registro no *ResultSet*.

6.2.4 Acesso a Base de Dados via Browser

O acesso a base de dados via *Browser* ocorre com a mesma utilização das classes citadas anteriormente. Porém, devido à política de segurança presente no Java, é necessário que se estabeleçam mecanismos para garantir a segurança.

A princípio, utilizando somente as classes com um acesso comum, as aplicações em Java não permitem acesso a base de dados via *browser* [69]. A esta política dá-se o nome de *SandBox*. Assim, para a utilização deste recurso, é necessário que se amplie esta política acrescentando permissões aos acessos.

As alterações das permissões ocorre através do programa *PolicyTool* , onde na sua execução há a chamada do arquivo de java.policy, que especifica as permissões dos códigos remotos.

6.3 Conclusão do capítulo

Neste capítulo procurou-se descrever algumas ferramentas que foram utilizadas no desenvolvimento deste trabalho. As conexões, estruturas e o funcionamento de elementos como a linguagem Java, a base de dados MySql, a estrutura do JDBC, entre outros foram algumas das questões discutidas.

7 Arquitetura DRM: Um Plug-in para Controle do Uso de Conteúdos Digitais

Este capítulo apresenta a proposta e o desenvolvimento da estrutura de uma arquitetura DRM. Entretanto, o trabalho tem como foco o aprofundamento dos aspectos relacionados com o desenvolvimento de um *plug-in* no lado do cliente.

7.1 Proposta de Arquitetura DRM

Através das pesquisas realizadas e que são descritas neste trabalho, procurou-se descrever uma proposta para arquitetura DRM. A tecnologia DRM busca soluções que possam disponibilizar e viabilizar a distribuição segura de conteúdos digitais.

A arquitetura demonstrada na figura 12 busca proporcionar maior segurança e diminuir as formas de distribuição ilegal dos conteúdos digitais, baseando-se no modelo XC2 da taxonomia proposta por [27].

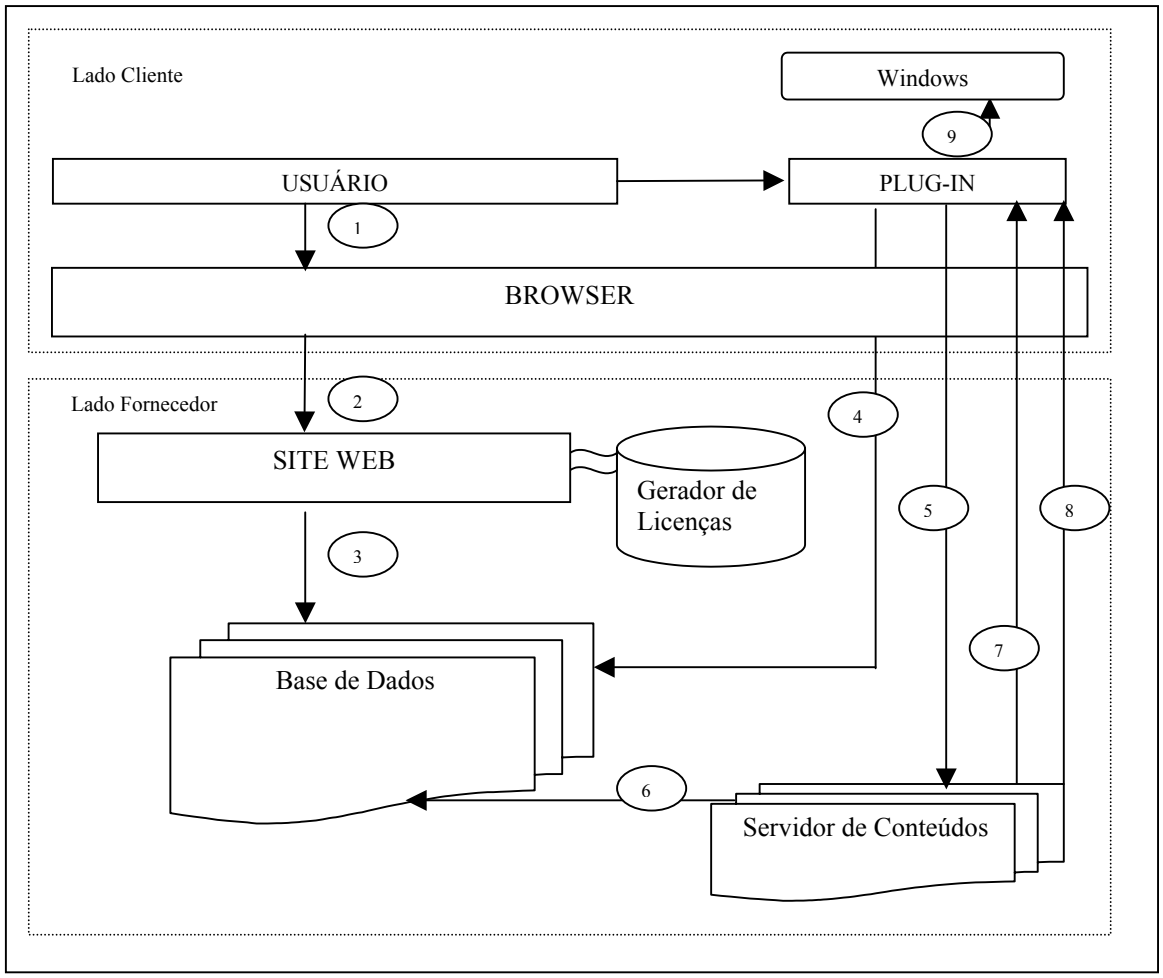


Figura 12 "Proposta de Arquitetura DRM".

Inicialmente o usuário acessa um *browser Web* (1). O *browser* faz a conexão com o *site web* que reside no lado do servidor (2). Após feita a conexão o usuário pode navegar na página e escolher o conteúdo e seus respectivos direitos, ou seja, como vai poder usufruir do conteúdo (3). Então o usuário pode abrir o *plug-in* para que o seus dados sejam confirmados (4). O *plug-in* solicita outras informações sobre licença e usuário para poder enviar ao servidor de conteúdos (5), que vai realizar uma confirmação das informações com a Base de dados (6). Confirmado, o servidor de conteúdos envia os direitos para o *plug-in* (7), e na seqüência envia o conteúdo (8). O *plug-in* está pronto para gerenciar o conteúdo e os direitos (9).

7.2 Discussão sobre Soluções de implementação

Nesta seção são discutidos alguns fatores de implementação e questões que foram sugeridas ao longo do trabalho, como possíveis pontos de pesquisa e discussão.

7.2.1 Definição dos direitos dos clientes e armazenamento

Este primeiro ponto de pesquisa esclarece algumas questões sobre os direitos. Os direitos são definidos pelo fornecedor do serviço, este é responsável em criar opções de direitos para que o usuário possa escolher qual direito se adapta com suas necessidades.

Estes direitos devem ser armazenados de forma segura no lado do cliente, para que o *plug-in* não necessite estar todo momento conectado a rede. Então o *plug-in* vai poder conferir os direitos sempre que necessário.

Existe a possibilidade de usar a técnica de ofuscamento de código para proteger os direitos. Ofuscamento de código é proteger o código fonte de determinados programas através de recursos computacionais e algoritmos criptográficos específicos [62].

7.2.2 Gerenciamento de licenças

Este gerenciamento é feito através do software *plug-in*, o gerador de licença tem a finalidade de produzir uma licença com as opções que o usuário escolheu no momento em que adquiriu um determinado conteúdo. Esta licença é baseada nos direitos do usuário, então o *plug-in* no lado do cliente é o responsável em gerenciar e fiscalizar através dos direitos como o usuário vai usufruir o conteúdo digital.

7.2.3 Desenvolvimento de *plug-in* cliente

O *plug-in* pode ser desenvolvido em qualquer linguagem capaz de descrever direitos para todos os tipos de conteúdo digital ou serviço. Outro fator relevante é a interoperabilidade com o sistema, pois o *plug-in* necessita de uma linguagem que possa interagir com os outros elementos da arquitetura, facilitando assim sua integração com a arquitetura estipulada. Um dos problemas encontrados durante o estudo, era como o *plug-in* faria a verificação dos direitos se estivesse desconectado da rede.

Então a opção em armazenar os direitos no lado do cliente é justificada pelo fator off-line, ou seja, não a necessidade que computador esteja conectado na rede toda vez em que o usuário solicite a abertura de um conteúdo. Com o intuito de dificultar a distribuição do documento, este é armazenado cifrado na máquina cliente, e a decifragem ocorre somente no momento em que o conteúdo é solicitado pelo usuário. Algo que pode ser considerado e estudado também é a proteção do conteúdo quando ele é carregado para a memória da máquina cliente.

7.2.4 Funcionamento do servidor de Conteúdo

O servidor de conteúdo é responsável em armazenar os documentos no lado do fornecedor de serviços, ponto de referência para efetuar o *download*. O *plug-in* inicia sua ligação com o servidor através do envio do número da licença e código do usuário, para que este confirme ou não com a base de dados quais informações o usuário deve receber. Como a maioria dos esforços se concentram no *plug-in*, as informações não são enviadas cifradas como algumas das sugestões dos trabalhos correlatos, opção esta que acaba gerando uma possibilidade de trabalho futuro.

7.3 Sugestões para implementação

O *site web* pode ser desenvolvido utilizando como base as linguagens JSP (*Java Server Pages*), A linguagem JSP possibilita a criação de páginas dinâmicas, interativas e de alto desempenho em uma rede internet ou intranet. Com as páginas JSP, os scripts são executados no servidor e não no cliente, sendo assim é o próprio servidor que transforma os *scripts* em HTML padrão, fazendo com que qualquer *browser* do mercado seja capaz de acessar um *site* que utiliza JSP. Devido a estas linguagens, a aplicação pode armazenar dados que são mantidos durante toda uma sessão, desta forma, os usuários podem, por exemplo, fornecer seu nome somente uma vez em uma página, sendo que as demais páginas podem obter este dado automaticamente. Este recurso é ideal para aplicações de comércio eletrônico pela Internet.

A Base de dados MySQL, tem como propósito armazenar os dados e proporcionar a manutenção dos registros armazenados.

A estrutura do *plug-in* pode ser implementada utilizando os conceitos de orientação a objetos, e linguagem Java com suas diversas classes e pacotes. Entre os pacotes destaca-se o pacote de segurança JCE - Java *Cryptography Extension,* que auxiliou na criptografia do conteúdo utilizando o algoritmo DES – *Data Encryption Standard.*

O Gerador de Licença pode ser totalmente desenvolvido através de XrML, pois a mesma linguagem vem se destacando na geração de licenças. O gerador pode receber informações essenciais do *site web*: Nome do usuário, número de licença, código dos direitos e permissões entre outras. Tem como uma de suas finalidades montar uma licença e liberar a impressão para o usuário.

7.4 Resultados de implementação

Esta seção descreve os resultados de implementação obtidos neste trabalho. Inicialmente é descrito um diagrama de caso de uso do protótipo desenvolvido. Na seqüência esta seção descreve o desenvolvimento do plug-in.

7.4.1 Diagrama de casos de uso

Nesta modelagem foram observados oito casos de uso (figura 13), que são descritos a seguir:

a) Conecta
b) Inicia transação (Usuário inicia uma transação que envolve a busca por um documento).
c) Cadastra (Usuário cadastra-se com seu dados)
d) Grava cadastro (executa uma operação de gravação onde as informações são enviadas para a base de dados).
e) Usuário abre o *plug-in* e (entra com *login* e senha)
f) Usuário envia informações para servidor de conteúdo (número de licença e código do usuário).
g) Consolida transação (*Plug-in* ao lado do cliente recebe as informações).

h) Finaliza transação (Usuário executa operação de fechamento do sistema ou nova busca).

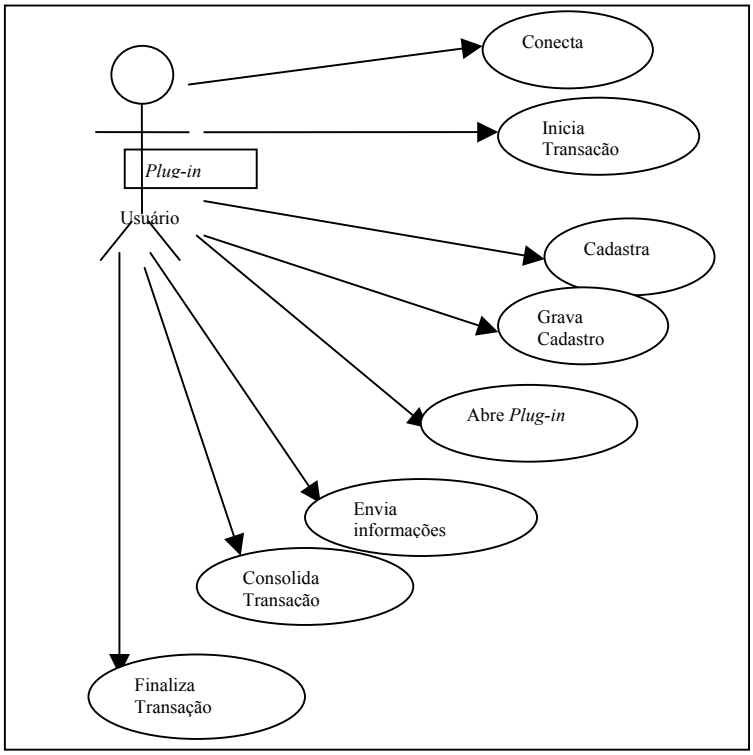


Figura 13 "Diagrama de Caso de uso".

7.4.2 Desenvolvimento do plug-in

O *plug-in* ao ser iniciado apresenta a seguinte *interface*:

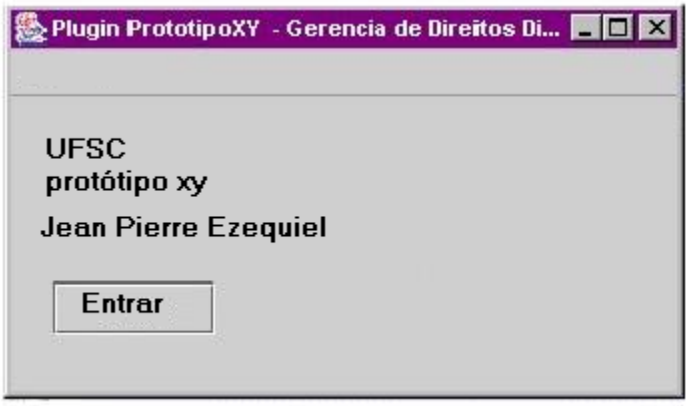
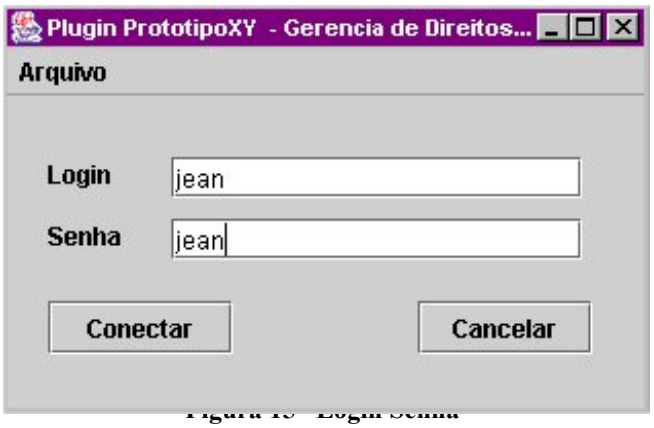


Figura 14 "Interface Inicial Protótipo xy"

Um dos primeiros passos foi elaborar um documento para ser transmitido, ou seja, documento sobre o qual o cliente comprou direitos digitais, para isto foi utilizado um arquivo texto simples. Uma página fornece o cadastro de clientes e a compra de direitos sobre os arquivos.

Foi criado também um conector de autenticação, porta pela qual o *plug-in* se conecta para que aconteça a autenticação do cliente, e recebimento do número da conexão pelo mesmo. Foi usado um *SocketServer*, TCP/IP.



A figura 15, demonstra a *interface* de autenticação com a base de dados onde é solicitado o *login* e senha (passo 4). Os dados da conexão são usados para gerenciar a sessão aberta pelo *plugin*.

```
private void btnConectarMouseClicked(java.awt.event.MouseEvent evt) {
        user = new Usuario();
        user.setLogin(jTextField1.getText());
        user.setPassword(jTextField2.getText());
        cc.setUsuario(user);
        cc.autenticar();
}
```

Um Autenticador, recebe um objeto *usuario* e faz a verificação se o mesmo é válido, se for válido retorna um número de conexão para o *plugin*.

Outro elemento desenvolvido é o conector de dados, este é responsável pela conexão do *plug-in* ao serviço de dados utilizando um número de conexão existente.

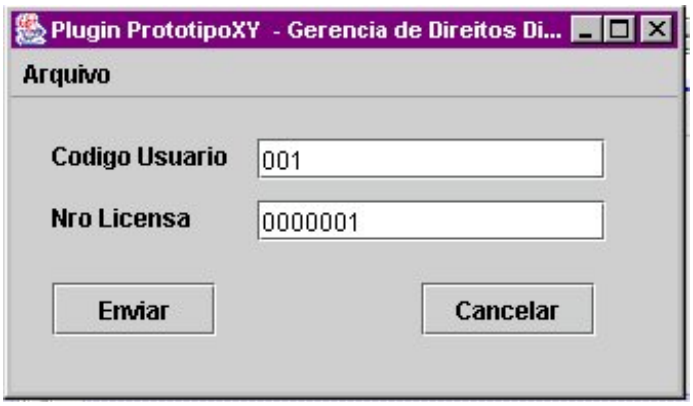


Figura 16 "Licença"

A figura 16, define a conexão com os dados necessários para o *download* do arquivo e efetua o mesmo.

```
private void btnEnviarMouseClicked(java.awt.event.MouseEvent evt) {
        cc.setItemConexao(item);
        cc.baixarArquivo();
           }
```

O Servidor de Dados quando receber um número de conexão esperado carrega os direitos e os transmite para o *plug-in*, logo depois carrega o conteúdo e transmite o arquivo para o *plug-in*. Para que haja uma comunicação deve existir uma Camada de acesso a dados – que vai ter a finalidade de atender as solicitações de dados gravados na Base de Dados MySql, feitos pelo programa.

Figura 17 "Impressão"

A figura 17 apresenta uma *interface* do *plug-in* responsável por abrir os documentos e gerenciar os direitos sobre os arquivos. Esta abre o arquivo cifrado e exibe para leitura, de acordo com o tipo de direito comprado possibilitando ou não impressão. O código abaixo demonstra o momento que ocorre a inicialização da cifragem dos dados no *plug-in*.

```
private void mnAbrirActionPerformed(java.awt.event.ActionEvent evt) {
      StringBuffer doc=null;
      this.abrirDireitos();

      this.gravarDireitos();
      if((this.NroVezes == -1) || (this.NroVezes > 0)){
         try{
```

Em casos onde o cliente escolhe por duas cópias de um mesmo conteúdo, mas que se destinam a estações diferentes, o *download* pode ocorrer em qualquer *host* que contenha o *software plug-in.* O usuário conclui o *download* na primeira estação escolhida, então solicita uma autenticação no segundo *host,* através do login e senha, número de licença e código do usuário. Então ocorre o processo de verificação dos dados, onde serão confirmados ou não. Se houver queda da conexão no momento em que ocorre o *download*,

deverá ser solicitada uma nova autenticação através do *plug-in,* para que o processo seja reiniciado.

7.4.3 Evolução do trabalho

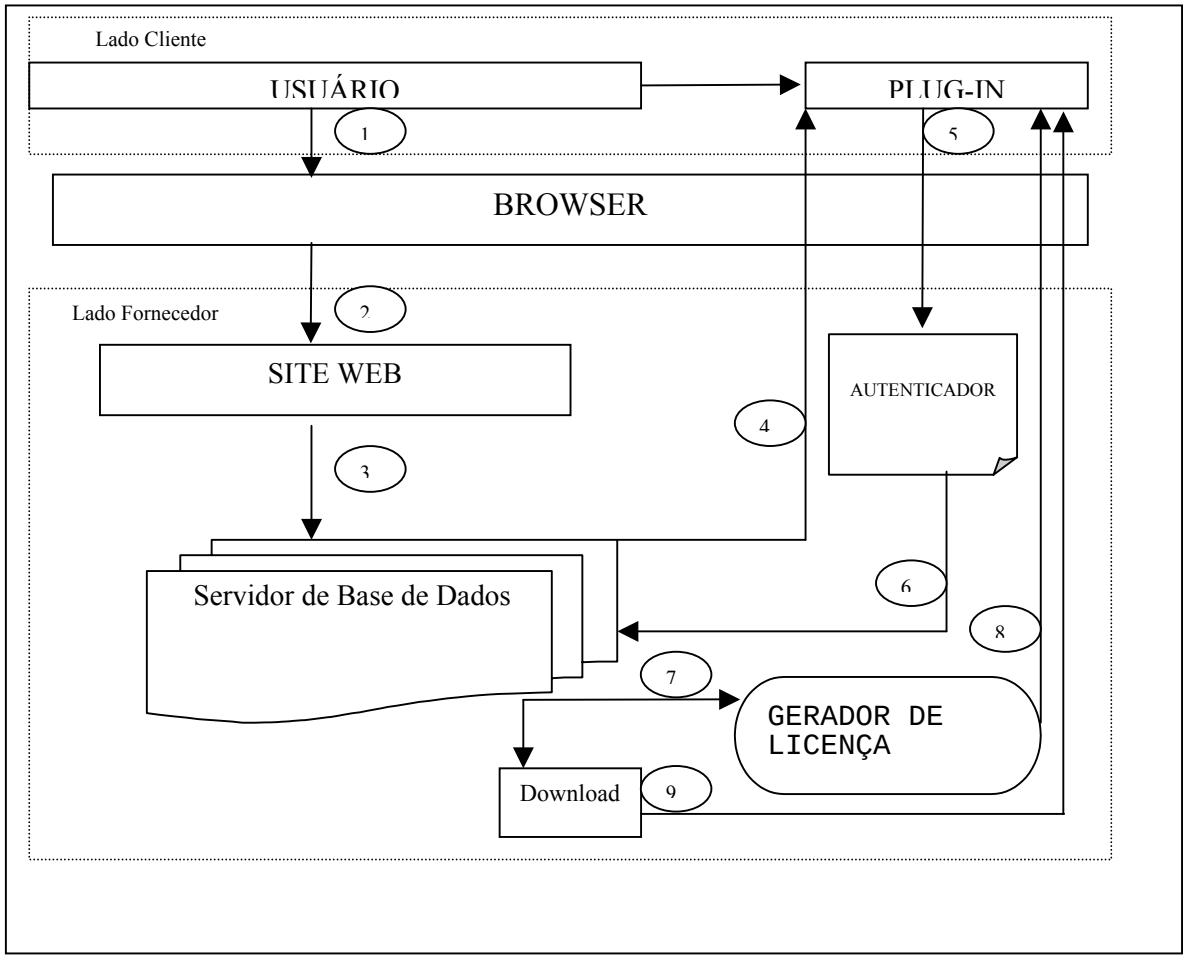


Figura 18 "Arquitetura inicial TI"

Com o decorrer da implementação detectou-se algumas falhas na arquitetura inicial, e também ocorreu algumas mudanças referentes ao posicionamento de alguns elementos.

Uma das falhas refere-se a comunicação do banco de dados com o lado cliente, pois nesta figura 18 a base de dados envia informações ao *plug-in* (passo 4), enquanto na nova arquitetura é o *plug-in* que solicita informação a base de dados (passo 4 da figura 12). Então optou-se por um banco de dados passivo, somente sofrendo ações não podendo enviar dados ao computador cliente, ocasionando maior segurança e agilidade.

Por motivos de segurança os applets não possuem permissão de gravar ou alterar arquivos no computador de quem os acessar, porém se forem applets seguros, ou seja, que apresentem certificados, esta operação pode ocorrer. O estudo dos certificados ainda não foi realizado, pois pretende-se integrar alguns elementos desta arquitetura com outros trabalhos que irão dispor a certificação. Ainda com o objetivo de melhorar a segurança, agilidade e comunicação entre os elementos, foi acrescentado um servidor de conteúdos. Na primeira arquitetura figura 18, é proposto que o conteúdo fique armazenado junto com os dados cadastrais (senha, login entre outros), já a nova estrutura propõe um local específico para armazenamento no lado fornecedor, o servidor de conteúdos. Outra mudança é o posicionamento do gerador de licenças, que ficava localizado no passo sete da arquitetura antiga, o que ocasionava uma difícil interação com outros elementos, como por exemplo na formação dos direitos. Agora após a mudança, no momento em que o usuário escolhe sua opções de utilização sobre o conteúdo (escolha dos direitos), o gerador de licença já recebe as informações e não necessita que a base de dados envie, o que também acaba justificando a troca da base dados citada no parágrafo anterior.

7.5 Conclusão do capítulo

Este capítulo compreende a junção de vários tópicos que formaram uma descrição da Estrutura de Uma Arquitetura para *Digital Rights Management* e também o desenvolvimento de um *Plug-in* para Controle de Uso de conteúdos Digitais. Foi demonstrado alguns passos da implementação bem como respectivas *interfaces* do *plug-in*.

Entre os tópicos descritos neste capítulo pode-se encontrar soluções para pontos de pesquisa que foram levantados em todo o trabalho e sugestões de implementação para os elementos da arquitetura proposta.

8 Conclusão

A partir deste trabalho pode-se comprovar que a tecnologia *Digital Rights Management* oferece amplo campo de estudo, para pesquisadores que desejam contribuir nos trabalhos que visam controlar a disseminação de conteúdos digitais. Atualmente a preservação da integridade dos conteúdos digitais e do *copyright* vem despertando o interesse da comunidade científica como pode ser concluído por meio deste trabalho. Com a elaboração da arquitetura, do protótipo de um *plug-in* e através dos estudos realizados, observou-se que o gerenciamento dos direitos digitais pode oferecer a segurança necessária para a distribuição de conteúdo via rede.

O protótipo desenvolvido neste trabalho e demonstrado no capítulo sete oferece entre suas características e diferenciais, uma solução no armazenamento das informações, estas são mantidas cifradas e "escondidas" no disco do cliente. A decifragem dos dados ocorre somente no momento em que o *plug-in* abre o conteúdo, para dificultar ainda mais, foi elaborada uma extensão para o arquivo, onde somente o *software* gerenciador reconhece.

Um dos objetivos gerais proposto no início do trabalho foi descrever uma Arquitetura para controle da disseminação de conteúdo digital, e também implementar o protótipo de um *plug-in* para o gerenciamento dos direitos e do conteúdo.

8.1 Contribuições Principais

Dentre as principais contribuições destacam-se:

a) O local onde os direitos são armazenados (Lado cliente no disco rígido);
b) O local onde o conteúdo é armazenado (Lado cliente no disco rígido);
c) Como são armazenados os direitos e o conteúdo (Armazenados cifrados e com extensão diferente onde somente o *plug-in* pode abrir);
d) Como ocorre o gerenciamento dos direitos e do conteúdo;
e) A proposta de uma nova arquitetura;
f) O funcionamento do *plug-in*;
g) A sugestão para implementação dos elementos da arquitetura.

8.2 Visão geral do trabalho

Através de várias pesquisas este trabalho procurou abordar diferentes conceitos, entre eles conceitos básicos de segurança, incluindo mecanismos e fundamentos. Também descreve alguns meios existentes de distribuição de conteúdo digital pela rede, bem como suas características e diversos exemplos. O estudo sobre a tecnologia *Digital Rights Management* é um dos focos que fundamentaram todos os esforços deste trabalho do início ao fim, sempre utilizando trabalhos relacionados como centro das justificativas.

A descrição de ferramentas e linguagens para implementação contribuíram para o desenvolvimento da Arquitetura e implementação de um protótipo *plug-in*, onde ambos possuem como finalidade principal contribuir para a evolução da tecnologia DRM contra a distribuição ilegal de conteúdos digitais pela rede.

8.3 Perspectivas futuras

Durante a realização deste estudo, e através dos resultados obtidos, surgiram algumas possibilidades de continuidade deste trabalho, dentre as quais pode-se identificar:

a) Evolução do *plug-in* para a leitura de arquivos de áudio e vídeo;
b) Inclusão de novas funcionalidades de acordo com a necessidade de utilização;
c) Evoluir para outra ferramenta de banco de dados, capaz de oferecer maiores recursos;
d) Desenvolvimento de uma biblioteca virtual, que possa fornecer diversos tipos de conteúdos digitais para distribuição segura mantendo sempre os direitos do copyright;
e) Uso de técnicas de ofuscamento de código para proteger os direitos armazenados no lado do cliente, bem como o próprio código executável do *plug-in.*
f) Geração de uma *watermark* (marca d'água), que identifique o serviço, o conteúdo e o *plug-in* responsável pelo gerenciamento.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] LANDWEHR,C. "***Computer Security"***, International Journal of Information Security, vol.1,n.1 pp. 2-13, issn 1615-5262, Springer-Verlag,2001.

[2] DONALD, L.; BRINKLEY; R. ***"Concepts and Terminology for Computer Security".*** Essay 2, In: Information Security: An Integrated Collection of Essays. Edited by Marshall D. Abrams, Sushil Jajodia, Harold J. Podell. IEEE Computer Society Press, Los Alamitos, California, USA, January 1995. Disponível em: http://www.acsac.org/secshelf/book001/book001.html. Acesso em 12/10/2002.

[3] BAILEY D. ***"A Philosophy of Security Management".*** Essay 3, In: Information Security: An Integrated Collection of Essays**.** Edited by Marshall D. Abrams, Sushil Jajodia, Harold J. Podell. IEEE Computer Society Press, Los Alamitos, California, USA, January 1995.

[4] BAILEY D.; ABRAMS, M. ***"Abstraction and Refinement of Layered Security Policy"***. Essay 5, In: Information Security: An Integrated Collection of Essays. Edited by Marshall D. Abrams, Sushil Jajodia, Harold J. Podell. IEEE Computer Society Press, Los Alamitos, California, USA, January 1995.

[5] OLSON, M.; ABRAMS, M. ***"Information Security Policy"***. Essay 7, In: Information Security: An Integrated Collection of Essays**.** Edited by Marshall D. Abrams, Sushil Jajodia, Harold J. Podell. IEEE Computer Society Press, Los Alamitos, California, USA, January 1995.

[6] PODELL, H. J. ***"Representative Organizations That Participate in Open Systems Security Standards Development".*** Essay 10, In: Information Security: An Integrated Collection of Essays. Edited by Marshall D. Abrams, Sushil Jajodia, Harold J. Podell. IEEE Computer Society Press, Los Alamitos, California, USA, January 1995.

[7] ABRAMS, M.; PODELL, H. J. ***"Supporting Policies and Functions".*** Essay 13, In: Information Security: An Integrated Collection of Essays. Edited by Marshall D. Abrams, Sushil Jajodia, Harold J. Podell. IEEE Computer Society Press, Los Alamitos, California, USA, January 1995.

[8] ABRAMS, M.; PODELL, H. J. ***"Cryptography"***. Essay 15, In: Information Security: An Integrated Collection of Essays**.** Edited by Marshall D. Abrams, Sushil Jajodia, Harold J. Podell. IEEE Computer Society Press, Los Alamitos, California, USA, January 1995.

[9] DODIS, Y.; FAZIO N. **"*Public Key Broadcast Encryption for Stateless Receivers"***. Computer Science Department, New York University, ACM Workshop on Digital Rights Management, USA, November 2002.

[10] GOLLMANN, D. **"*Computer Security*"**, 336 pages ; Publisher: John Wiley & Sons Ltda; I edition England, February 16, 1999. ISBN: 0-471-97844-2

[11] AMOROSO, E. **"*Fundamantals of Computer security technology*"**, Upper Saddle River Prentice Hall International Editions, New Jersey 1994. ISBN: 0-13-108929-3

[12] RUGGLES, T. ***"Comparison of Biometric Techniques"***. February 11, 2001 Disponível em: http://biometric-consulting.com/bio.htm. Acesso em: 15/05/2003.

[13] POLEMI, D. **"*Review and evaluation of Biometric Techniques for Identification and Authentication - Final Report*"**. 3 May 1999. published by DG Information Society of the European Commission. **INFOSEC - Security of Telecommunications and Information Systems,** Disponível em: http://www.cordis.lu/infosec/src/stud5fr.htm. Acesso em: 18/05/2003.

[14] CLARKE, R. ***"Human Identification in Information Systems"*** Published in Information Technology & People 7,4 (December 1994) 6-37, Disponível em: http://www.anu.edu.au/people/Roger.Clarke/DV/HumanID. Acesso em 15/03/2001.

[15] STALLINGS, W. **"Protect Your Privacy"**, Englewood Cliffs (New Jersey, USA), Prentice Hall, (1995). ISBN 0-13-185596-4

[16] SANDHU, R.; SAMARATI, P. ***"Access Control: Principle and Practice,"*** *IEEE Communications Magazine,* vol. 32, pp. 40 - 48, September 1994.

[17] HEADY, R.; LUGER, G.; MACCABE, A. ***"The Architecture of a Network Level Intrusion Detection System".*** Technical Report CS90-20, Department of Computer Science, University of New Mexico, August 1990.

[18] FAQ: ***"Network Intrusion Detection Systems"*** Disponível em: http://www.robertgraham.com/pubs/network-intrusion-detection.html. Acesso em 21/03/2003.

[19] MACLACHLAN, M. ***"Time is coming for Digital Rights Management"***, Framingham, USA, Set, 2001. Disponível em: http://www.itworld.com/nl/ebus_trends/09202001/ Acesso em 5/03/2003.

[20] SANDER, T. ***"Golden Times Rights Management",*** USA 2001, pp. 1-12 [online]. The Law e Technology of DRM Conference, Fevereiro 2003 Disponível em: http://citeseer.nj.nec.com/489047.html. Acesso em 09/06/2003.

[21] DUHL, J.; KEVORKIAN, S. ***"Understanding DRM Systems"***, InterTrust Inc., IDC White Paper, Framingham, MA, USA, 2001, pp. 1-13. Disponível em: http://www.intertrust.com

[22] GUNTER, C.; WEEKS, S.; WRIGHT, A. ***"Model and Languages for Digital Rights"***, Intertrust Star Lab, Santa Clara, CA, USA, 2001/ 34th Annual Hawaii International Conference on System Sciences (HICSS-34)-Volume 9, pag.9076, January 2001.

[23] SCHMELZER, R. ***"ContentGuard XrML - Protecting Digital Resources with XrML"***, Waltham, USA, Dec, 2001. Disponível em: http://www.xrml.org/Reference/ContentGuard_XrML_Zapthink.pdf / Acesso em 02/07/2003.

[24] IANELLA, R. ***"Open Digital Rights Management Architectures"***, D-Lib Magazine,Vol. 7, Jun, 2001.

[25] IANELLA, R. ***"Open Digital Rights Management"*** W3C Digital Rights Management Workshop, France, 2001.

[26] IANNELLA, R. ***"Digital Rigths Management (DRM) in Education - The Need For Open Standards"***, Paper IEEE LTSC, Expression Language Study Group Workshop, Jun, 2002.

[27] PARK, J.; SANDHU, R.; SCHIFALACQUA, J. ***"Security Architectures for Controlled Digital Information Dissemination"***, ISE Departament, Proceedings of the 16thAnnual Computer Security Applications Conference, December, USA 2000.

[28] CHOW, S.; EISEN, P. ***"A White-Box Des Implementation for DRM Applications"*** Carleton University, ACM Workshop on Digital Rights Management, Washington DC, USA, November , 2002.

[29] NAGRA, J.; THOMBORSON, C. ***"A Functional Taxonomy for Software Watermarking"*** Depart. of Computer Science, New Zealand, Computer Science Conference ACSC, 2002.

[30] KIROVSKI, D.; PETITCOLAS, F. ***"Replacement Attack on Arbitrary Watermarking Systms"***, Microsoft Research Technical Report, Cambridge, USA, ACM Workshop on Digital Rights Management, 2002.

[31] FEIGENBAUM, J.; FREEDMAN, M.; SANDER, T.; SHOSTACK A***.,"Privacy Engineering for Digital Rights Management Systems",*** Dep Sciencce,Yale University,New Haven, USA. ACM Workshop in Security and Privacy in Digital Rights Management, 2001.

[32] FAQ: ***"Frequently Asked Questions"*** Disponível em: http://www.xrml.org/faq.asp. Acesso em 29/10/2002.

[33] STANDARDS: ***"Reference Materials"*** Disponível em: http://www.xrml.org/reference.asp. Acesso em 17/11/2002.

[34]Microsoft Windows Media TUTORIALS: ***"DRM"*** Disponível em: http://www.microsoft.com/windows/windowsmedia/wm7/drm/tutorial.asp.Acesso em 22/11/2002.

[35] TEMPLATE:***" ContentGuard, Inc. Marks its Spin-off From Xerox with Microsoft Alliance and XrML Standards Initiative"*** Disponível em: http://www.xerox.com/go/xrx/template. Acesso em 22/11/2002.

[36] Xerox FAQ, ***"The Open Digital Rights Language Initiative"*** Disponível em: http://www.xerox.com/go/xrx/template. Acesso em 23/11/2002.

[37] Accenture Company ***"Market of the Digital Products"*** Disponível em: http://www.accenture.com/xd/xd.asp?it=enweb&xd=aboutus\about_home.xml. Acesso em 20/03/2003.

[38] DOI***"Content Directions, Inc. Use the Digital Object Identifier..."*** Disponível em: http://www.doi.contentdirections.com/DOI-EB-Demo/mhindex.htm. Acesso em 12/03/2003.

[39] Cross ***"Linking bright ideas together"*** Disponível em: http://www.crossref.org./09demo/index.html. Acesso em 13/03/2003.

[40] Ebrary Tools ***"Linking bright ideas together"*** Disponível em: http://www.ebrary.com/technology/infotools.jsp. Acesso em 15/03/2003.

[41] JORDAN, C.; CHONGY, N.; BUURENZ, R.; HARTELY, P.; KLEINHUIS, G. ***"Security Attributes Based Digital Rights Management"*** Workshop on Interactive Distributed Multimedia Systems pages 339--352, Springer-Verlag, Berlin, Nov 2002.

[42] SELLARS, D. ***"An introduction to steganography"*** tech. rep., University of Cape Town, Computer Science/ 8th Annual Computer Security Applications Conference, pages 153-159 Disponível em: http://www.cs.uct.ac.za/courses/CS400W/NIS/papers99/dsellars/index.html. Acesso em maio/2003.

[43] MULLIGAN, D.; BURSTEIN, A.; ERICKSON, J. ***"Supporting Limits on Copyright Exclusivity in a Rights Expression Language Standard"*** Samuelson Law, Technology & Public Policy Clinic; The Law & Technology of DRM Coference, August 13, 2002.

[44] COX, B***.; "Superdistribution Objects as Property on the Electronic Frontier"*** Reading, MA, Addison-Wesley Publishing Pub Company, 205 pages, 1st edition January, 1996 ISBN: 0201502089

[45] SANDHU, R.; PARK, J. ***"Towards Usage Control Models beyond Traditional Access Control"*** In: Proceedings of 7th ACM, Symposium on Access Control Models and Technologies, pp.57-64, jun.2002.

[46] SANDHU, R.; ***"Engineering Authority and Trust in Cyberspace: The OM-AM and RBAC way"***, Proceedings of the 5th ACM workshop on Role-Based Access Control, ACM, Berlin, July, 2000.

[47] IBM ***"New Rules e-commerce"*** Disponível em: http://www-1.ibm.com/mediumbusiness/sbcuk/feature_advice.jsp?id=412. Acesso em 25/03/2003.

[48] IBM ***"Frequently asked questions"*** Disponível em: http://www-1.ibm.com/mediumbusiness/sbcuk/feature_advice.jsp?id=4122. Acesso em 25/03/2003.

[49] GRESSENS, B.; BROUSSEAU, C. ***"The Value Propositions of Dynamic Pricing in Business-to-Business E-Commerce",*** 8th European Conference on Information Systems 2000, Disponível em: http://www.crmproject.com/documents.asp?d_ID=733#. Acesso em 23/03/2003.

[50] WANG, X.; LAO, G.; DE MARTINI, T.; REDDY, H.; NGUYEN, M.; VALENZUELA, E.; "***XrML - eXtensible Rights Markup Language"*** Proceedings of the 2002 ACM workshop on XML security, November, 2002.

[51] LEE, J.; SOHN, M.; ***"The eXtensible Rule Markup Language"*** Korea Advanced Institute of Science and Technology, Communications of the ACM, vol. 46, n. 5, 2003 May 2003.

[52] OASIS Rights Language Technical Committee, "***Rights Language".*** Disponível em: http://www.oasis-open.org/committees/rights. Acesso em 18/04/2003.

[53] BLUM, Renato. ***Opice - Direito Eletrônico.*** São Paulo: EDIPRO – Edições Profissionais, 2001.

[54] WEFFORT, F. "***Lei da Propriedade Intelectual".*** VirtualBooks, Formato: e-book/ PDF, Código: bvbCDlproint0001, 2001. Disponível em: http://virtualbooks.terra.com.br/freebook/codigos/intelectual.htm. Acesso em 11/05/2003.

[55] GANDELMAN, H. "***De Gutenberg a Internet: Direitos Autorais na Era Digital".*** São Paulo: Record, ISBN: 8501048771, Edição: 4, Páginas 333, Ano: 2001.

[56] CABRAL, A. ***"Nova Lei de Direitos Autorais".*** São Paulo: Harbra, ISBN: 852940257X Edição: 4, Páginas 190, Ano: 2003.

[57] ERICKSON, J. ***"Fair use, DRM, and trusted computing"*** Communications of the ACM, V.46, n.°, April 2003.

[58] IBM ***"Electronic Media Management System (EMMS)"*** Disponível em: http://www-3.ibm.com/software/data/emms. Acesso em 21/03/2003.

[59] FRIESEN, N.; MOURAD, M.; ROBSON, R.; ***"Towards a Digital Rights Expression Language Standard for Learning Technology",*** IEEE White Paper, A Report of the IEEE Learning Technology Standards Committee Digital Rights Expression Language Study Group. http://ltsc.ieee.org/meeting/200212/doc/DREL_White_paper.doc

[60] ISO/IEC. 15408-1: 1999 (E)- Part1: Introduction and general model.In: ***Information Technology – Security Techniques – Evolution Criteria for Security***, First edition, ISO/IEC, December 1999.

[61] LAMPSON, B; ***"Protection"*** . IN: 5th Princeton Symposium on Information Sciences and Systems, March 1971. Reprinted in ACM Operating Systems Review, v.8, n,1, p.18-24, 1974.

[62] WROBLEWSKI, G; ***"General Methodo os Program Code Obfuscation (Draft)"*** PhD Dissertation, Wroclaw University of Technology, Institute of Engineering Cybernetics, 2002.

[63] GONG, L; ***"Java Security:Present and Near Future"*** IEEE Magazine Micro, 17(3):14--19, May/June 1997.

[64] KOVED, L; PISTOIA, M; KERSHENBAUM, A; ***"Access Rights Analysis for Java"*** IBM T.J Watson Research Center, ACM SIGPLAN Notices, vol. 37, no. 11, p. 359-72, November 2002.

[65] BURTON, B; MAREK, V; ***"Applications of JAVA programming language to database management"***, Department of Computer Science University of Kentucky, ACM Press, Volume 27, Issue 1, Pages: 27 - 34 New York, NY, USA ,March 1998.

[66] Srinivas, R. N; ***"Security and Identity using Java",*** ACM, www2002 the eleventh international world wide web conference, Honolulu, Hawaii, USA, 7-11 May 2002.

[67] LEROY, X; ROUAIX F; ***"Security properties of typed apples"*** Proceedings of the 25th ACM SIGPLAN-SIGACT symposium on Principles of programming languages, January 1998.

[67] MySQL ***"MySQL Reference Manual"*** Disponível em: http://www.mysql.com/downloads/index.html, Copyright c° 1997-2003 MySQL AB Acesso em 28/09/2003.

[68] SOSONKIN, M; NAUMOVICH, G; MEMON, N; ***"Software and systems: Obfuscation of design intent in object-oriented applications"*** Proceedings of the 2003 ACM workshop on Digital rights management,October 2003.

[69] DEITEL, H; DEITEL, P; ***"Java, Como Programar".***Editora:Bookman, ISBN: 8536301236 , 4ª Edição, N^0 de páginas:1386, Ano: 2002.

[70] KURNIAWAN, B; ***"Java para a Web com Servlets, JSP e EJB"*** Editora: Ciência Moderna, ISBN: 8573932104 1ª Edição, N^0 de páginas: 832, Ano:2002.

[71] TAYLOR, A; BUEGE, B; LAYMAN, R; ***"Segurança Contra Hackers: J2EE e Java"*** Editora: Futura, ISBN: 8574131563 , 1ª Edição, N^0 de páginas: 456, Ano 2003.

[72] OAKS,S; ***"Segurança de dados em Java"*** Editora: Ciência Moderna, ISBN: 8573930403, 1ª Edição, N^0 de páginas: 433, Ano 1999.

[73] GOLDEN, J; POKLOP, L; TRANFAGLIA, S. ***"JAVA PROGRAMMING: PART 1"*** ZDU Student Manual, ISBN: 0-73725-349-5, Part number: ZDU56705, www.dct.ufms.br/~sfreitas/html/JAVA_book.PDF

[74] POTTS, A; FRIEDEL, D. ***"Java Programming Language Handbook"*** Editions: Paperback Coriolis Group, April 1, 1996. ISBN 1883577772. http://isbn.nu/1883577772

[75] HAROLD, E. ***"Java Network Programming, 2nd Edition"*** Publisher : O'Reilly, ISBN 1-56592-870-9, August 2000, 757 pages. http://safari.oreilly.com/?XmlId=1-56592-870-9

[76] Borland, A Division of Inprise Corporation ***"Developing Database Applications"***

[77] FAQ: ***"API On-line"*** Disponível em: http://java.sun.com/j2se/1.3/docs/api/index.html. Acesso em 25/10/2003.

[78] MySQL: ***"MySQL"*** Disponível em: http://mysql.com. Acesso em 18/10/2003.

[79] EZEQUIEL, P, J; WESTPHALL, M, C; ***"DRM – Em Busca da Perfeição Gerando o Aumento da Segurança Oferecida pela Web",*** III Congresso Brasileiro de Computação Itajaí - agosto 2003.

[80] EZEQUIEL, P, J; WESTPHALL, M, C; ***"Estrutura de uma Arquitetura para Digital Rights Management - DRM",*** II ECTEC - Encontro de Ciência e Tecnologia - Lages - outubro 2003.