Distribuição de Direitos de Acesso e Licenças para o Gerenciamento de Conteúdos Digitais

Cleber V. Filippin [1], Valério Rosset [1], Carla M. Westphall [2]

[1]Faculdades Integradas da Rede de Ensino Univest – FACVEST

[2]Universidade Federal de Santa Catarina - UFSC

{nemesis, valerio, carla}@lrg.ufsc.br

Abstract. *This article proposes an architecture for distributing and managing the digital contents, combining traditional access control and Digital Rights Management (DRM) aspects, which executes the content usage control. The architecture defines security policies to establish access rights to protected content and to establish licenses to control the use of digital contents at the client side. This work also defines models for the authorization and rights distribution entity and for the license creation, distribution and management entity. Prototypes are implemented using XML-based technologies, which facilitates the integration of different modules of the architecture.*

Resumo. *Este artigo propõe uma arquitetura de distribuição de direitos de acesso e licenças para o gerenciamento de conteúdos digitais, combinando aspectos de controle de acesso tradicional e Digital Rights Management (DRM), que executa o controle de uso do conteúdo. A arquitetura define políticas de segurança para estabelecer direitos de acesso a conteúdo protegido e para estabelecer licenças para controlar o uso de conteúdos digitais no lado cliente. Este trabalho também define modelos para a entidade de autorização e distribuição de direitos e para a entidade de criação, distribuição e gerenciamento de licenças. Protótipos são implementados usando tecnologias baseadas em XML, que facilitam a integração dos diferentes módulos da arquitetura.*

1. Introdução

O crescimento da *Internet* como meio de distribuição e a evolução das tecnologias digitais possibilita o surgimento de novos modelos e oportunidades de negócios para distribuição de conteúdos na forma digital. Entretanto, as formas tradicionais de controle de direitos sobre conteúdos como leis, contratos e criptografia, não são suficientemente eficientes para impedir ou diminuir o problema da distribuição ilegal de conteúdos digitais, trazendo a necessidade de desenvolvimento de modelos e tecnologias para gerenciamento, segurança, controle e automatização do fluxo de conteúdo e do acesso a serviços na *Internet* [Park et. al 2000].

O nível de proteção desejado vai além da simples segurança para a distribuição do conteúdo digital; é necessário que existam maneiras de fornecer uma proteção persistente do conteúdo, ou seja, proteção que permanece com o conteúdo depois deste ser transmitido [Erickson et al. 2001]. *Digital Rights Management* (DRM) é o termo comum associado com tecnologias capazes de proteger conteúdos digitais após a distribuição, proporcionando maneiras de exercer controle de uso sobre o conteúdo. Nos trabalhos existentes na literatura [Rosenblatt et al. 2002], [Chong et al. 2002], [Park et

al. 2000] e [Park and Sandhu 2002], existem propostas de alguns modelos para gerenciamento e controle *do acesso* e *do uso* dos conteúdos digitais. Entretanto, ainda existem várias questões sem solução, como a questão da interação entre o controle de acesso tradicional dos conteúdos digitais e o controle de uso, provida pelos modelos DRM. Nesse contexto, este artigo propõe uma arquitetura para distribuição de direitos e licenças para o gerenciamento de conteúdos digitais, unindo aspectos do controle de acesso tradicional e aspectos de DRM que realizam o controle de uso do conteúdo. A arquitetura trata os aspectos da autorização de acesso aos conteúdos, definindo a interação entre os componentes do controle de acesso e os componentes de controle de uso. Trata também da criação, da distribuição e do gerenciamento de licenças de uso dos conteúdos digitais.

O artigo está organizado da seguinte forma: a seção 2 apresenta uma visão geral sobre DRM e os trabalhos de pesquisa relacionados. A arquitetura para distribuição e gerenciamento de conteúdos digitais é apresentada na seção 3, definindo aspectos da autorização, da criação, distribuição e gerenciamento de licenças. Os protótipos desenvolvidos também são descritos na seção 3. Conclusões são apresentadas na seção 4.

2. Digital Rights Management (DRM)

DRM envolve a descrição, identificação, comercialização, proteção, monitoramento e rastreamento de formas de direitos de uso sobre conteúdos, incluindo o gerenciamento de relacionamentos entre detentores de direitos [Ianella 2001]. Soluções que possibilitam proteção persistente podem incluir componentes tecnológicos como empacotadores de conteúdo, controladores, servidores de licenças, rastreamento de acesso ou de uso de conteúdo, e licenciamento de direitos [Rosenblatt et al. 2002]. Sistemas DRM fornecem proteção persistente e gerenciam o conteúdo, baseados em regras de uso especificadas pelo proprietário ou distribuidor do conteúdo, e nos direitos detidos pelo usuário.

Atualmente, existem diversas tecnologias e soluções criadas para atenderem objetivos e modelos de negócios no mercado de DRM. Tentativas de padronização incluem a linguagem de especificação de direitos XrML (*eXtensible rights Markup Language*) e o protocolo ICE (*Interchange Content Exchange*) [Rosenblatt et al. 2002]. Soluções proprietárias incluem soluções específicas para determinados formatos e modelos de negócios, e soluções mais abrangentes, que podem ser utilizadas com vários formatos e modelos de negócios. Mas soluções proprietárias são geralmente fechadas, e não especificam quais tecnologias são usadas, nem como são realizadas as tarefas de proteção de conteúdo e controle de uso, ou seja, não existem padrões que estabeleçam uma maneira específica para disseminar e controlar o acesso sobre conteúdos digitais.

2.1. Trabalhos de Pesquisa Relacionados

Trabalhos de pesquisa envolvem modelos e arquiteturas DRM, mas não são determinantes e esclarecer técnicas para implementar o controle sobre conteúdos digitais. Em [Chong et al. 2002] é apresentado o projeto SUMMER (*SecUre MultiMedia Retrieval*), que envolve apenas uma arquitetura fim-a-fim para gerenciamento de bases de dados multimídia, envolvendo duas partes distintas, uma para identificação, autenticação, autorização; outra parte para executar funções de servidor de licenças. Em [Rosenblatt et al. 2002] é proposta uma arquitetura de referência para soluções DRM, composta por três elementos principais: o servidor de conteúdo, o servidor de licenças e o cliente. [Park et al. 2000] analisa a disseminação controlada de informação digital, apresentando uma taxonomia de arquiteturas de segurança baseadas em três fatores principais: máquina virtual, conjunto de controle e estilo de distribuição.

No trabalho de pesquisa em [Park and Sandhu 2002], a noção de controle de uso (*Usage Control* - UCON) é apresentado e unido com a noção de ORCON (*Originator Control*), um mecanismo de controle de acesso baseado em políticas.

Nos trabalhos de pesquisa analisados, percebe-se a necessidade de pesquisas mais aprofundadas em relação a aspectos como autorização e sistemas DRM. Existe a necessidade de análise de mecanismos e soluções, e de estudos buscando soluções para problemas como o controle e gerenciamento de licenças. Modelos e arquiteturas que permitam implementar na prática os aspectos de controle de acesso e de uso não são encontrados nos trabalhos de pesquisa analisados.

3. Arquitetura de Gerenciamento e Distribuição de Conteúdos Digitais

A arquitetura para gerenciamento e distribuição de conteúdos digitais (*Digital Content Distribution and Management Architecture* – DCDMA) apresentada neste artigo apresenta uma divisão e distribuição dos elementos DRM básicos em entidades mais especializadas. A arquitetura (Figura 1) é formada pelas entidades definidas como: Entidade Cliente (*Client*); Entidade de Autenticação (*Authentication Entity* - AE); Entidade de Conteúdo (*Content Entity* - CE); Entidade de Criação, Distribuição e Gerenciamento de Licenças (*License Creation, Distribution and Management Entity* - LCDME); e Entidade de Autorização e Distribuição de Direitos (*Authorization and Rights Distribution Entity* - ARDE).

A *Entidade Cliente* (*Client*) executa o controle de acesso aos conteúdos digitais protegidos através de licenças de uso. Ela é definida como uma aplicação de controle de conteúdo que é executada no lado cliente como um *plugin*.

A *Entidade de Autenticação* (AE) é responsável por recolher as informações necessárias para autenticar um usuário, e disponibilizar uma credencial do usuário para os outros componentes do sistema, funcionando como uma base de informações de atributos de usuários. A *Entidade de Conteúdo* (CE) é responsável por distribuir conteúdos protegidos aos usuários autenticados no sistema, e serve também como base de informações de atributos de conteúdos protegidos e de informações relacionadas a pagamento e assinaturas.

A *Entidade de Criação, Distribuição e Gerenciamento de Licenças* (LCDME) é responsável por criar e distribuir licenças usadas para o controle de uso de conteúdos protegidos, e o gerenciamento de uso destas licenças. O processo de geração de licenças é feito com base nos direitos que o usuário possui sobre os conteúdos digitais protegidos. Esses direitos são determinados através da avaliação de políticas de controle de acesso durante o processo de autorização. A *Entidade de Autorização e Distribuição de Direitos* de acesso (ARDE) é responsável por avaliar políticas de controle de acesso e determinar quais os direitos que o usuário possui sobre um conteúdo digital protegido específico, e disponibilizá-los ao servidor de licenças.

A interação entre as entidades pertencentes à arquitetura DCDMA ocorre através de trocas de mensagens seguras. Os usuários exercem os direitos de acesso especificados por licenças, através de ações requisitadas a partir de uma aplicação de leitura, visualização ou execução de conteúdos digitais.

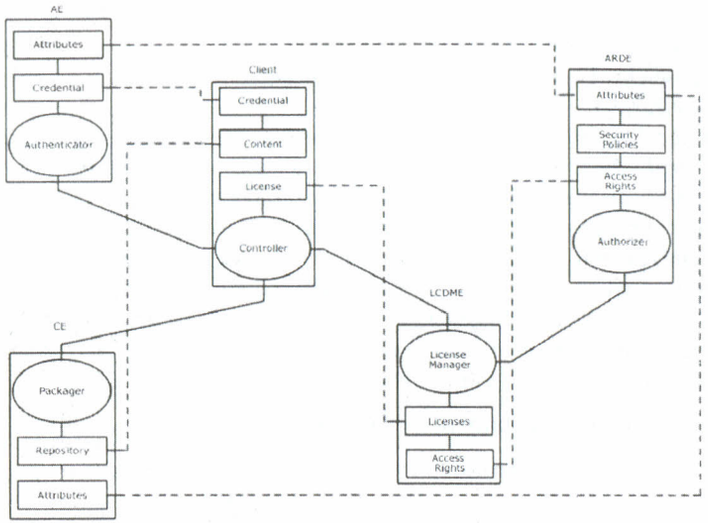

Figura 1– Arquitetura DCDMA

Este artigo apresenta a definição das entidades ARDE e LCDME, e aborda suas estruturas internas, comunicação e implementação dos protótipos.

3.1. Modelo da Entidade de Autorização e Distribuição de Direitos de Acesso

A entidade de autorização e distribuição de direitos é subdividida em componentes responsáveis por disponibilizar as políticas de segurança e atributos necessários para o processo de decisão, bem como componentes diretamente responsáveis pelo processo de decisão.

A definição de entidades envolvidas no processo de autorização como suporte a efetivação da arquitetura proposta é baseada no RFC-2904 *AAA Authorization Framework* da IETF [Vollbrecht 2000], que determina a distribuição de componentes em uma arquitetura de autorização genérica. A utilização desses componentes (individualmente ou em conjunto) de maneira distribuída representando as entidades da arquitetura proposta permite a não sobrecarga em uma entidade específica. O *AAA Authorization Framework* da IETF define os seguintes componentes: o PEP (*Policy Enforcement Point*) é o componente responsável por requisitar e aplicar decisões de acesso sobre algum recurso; o PDP (*Policy Decision Point*) é o componente responsável por avaliar requisições de acesso através de políticas de segurança e determinar se a requisição de acesso a um recurso é válida ou não; o PIP (*Policy Information Point*) é responsável por fornecer ao PDP valores de atributos de usuários, dos recursos e do ambiente; o PAP (*Policy Administration Point*) é responsável por criar e armazenar políticas de segurança; e o PRP (*Policy Retrieval Point*) é responsável por fornecer as políticas de segurança ao PDP.

O *AAA Authorization Framework* da IETF é bastante flexível e permite implementar a autorização de forma distribuída e independente, sendo que a interação e organização entre os vários pontos são de responsabilidade do desenvolvedor. Esse *framework* foi utilizado também como base no modelo da linguagem para definição de políticas de segurança designada XACML (*eXtensible Access Control Markup Language*) [Godik 2003].

Na DCDMA, a entidade ARDE é implementada através de uma aplicação de autorização e distribuição de direitos de acesso (ARDA), que possui em sua estrutura interna componentes que realizam as mesmas funcionalidades do PDP, e PRP. Da mesma maneira a entidade LCDME pode ser vista como o PEP. O conceito de PAP é abstraído nesta arquitetura. Já o PIP pode estar presente em todas as entidades, devido ao fato da necessidade de troca de informações sobre atributos entre elas.

O uso dos padrões baseados em XML, que são aplicados para estabelecer a geração e troca de informações seguras entre as entidades distribuídas (Figura 2), acrescenta ao modelo DCDMA características de flexibilidade e interoperabilidade não encontradas em outras arquiteturas. Efetivamente esses padrões não fazem parte da arquitetura, mas o uso desses padrões pode tornar desnecessária a criação de protocolos de segurança específicos para uma arquitetura distribuída.

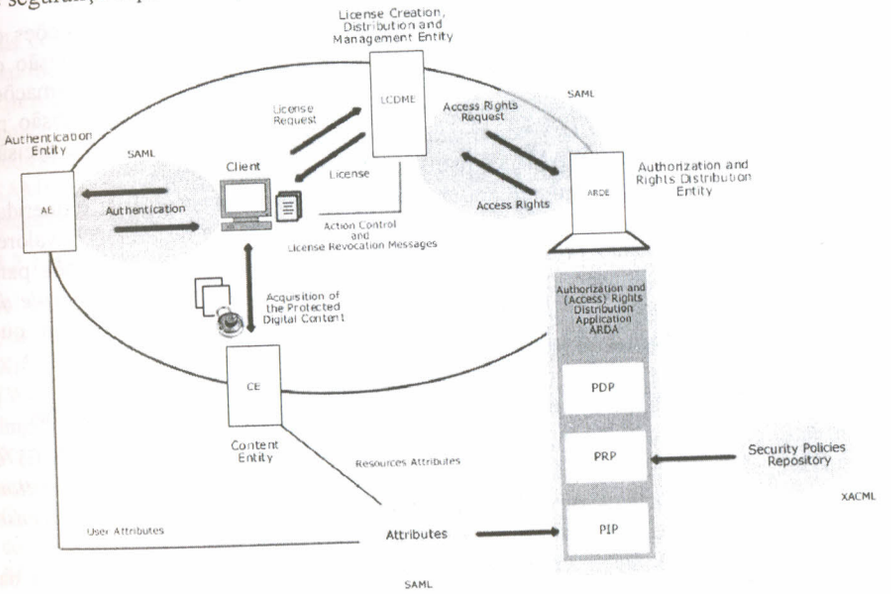

Figura 2 – DCDMA, ARDE e Padrões de segurança XML.

As trocas de mensagens de autorização e distribuição de direitos de acesso são implementadas através do uso do padrão de segurança SAML (*Secure Assertion Markup Language*) [Maler 2003]. As políticas de segurança são implementadas através do uso do padrão de segurança XACML (*eXtensible Access Control Markup Language*) [Godik 2003]. É visível que apenas SAML e XACML não garantem a integridade e autenticidade de mensagens, apenas fornecem vocabulários para estabelecer requisições e respostas para asserções de decisões de acesso, autenticação, atributos e definição de políticas respectivamente. Assim, para reforçar a segurança na troca de mensagens entre as entidades pode-se utilizar outros padrões de segurança XML.

3.1.3. Implementação da Entidade ARDE

O protótipo foi desenvolvido como um *framework* para aplicações *Java*, e contém as diversas classes que representam os diferentes módulos da estrutura para uma aplicação

ARDA. A implementação dessas classes permite que outras aplicações possam utilizá-las de maneira individual. Assim, desenvolvedores podem utilizar as classes de maneira a implementar a melhor solução para suas necessidades. Os pacotes utilizados para desenvolvimento foram o *OpenSAML* [Opensaml 2002] versão 1.0, *SunXACML* [Sunxacml 2003] e o *parser Xerces*.

O protótipo implementado determina como será o acesso a todos os conteúdos que estarão sob domínio dos usuários. O processo de autorização é executado por uma aplicação de *middleware*. Uma aplicação de autorização e distribuição de direitos de acesso (ARDA) é dividida em diferentes módulos que executam as funções referentes ao PDP, PRP e PIP, além de outros módulos responsáveis por receber, enviar e formatar mensagens. A estrutura da aplicação ARDA é formada pelos módulos *Listen/Response*, *Encapsulamento*, *Desencapsulamento*, *Recuperação de Políticas*, *Recuperação de Atributos* e *Controle de Decisão*.

O módulo *Listen/Response* é responsável pelo recebimento de requisições de autorização sobre direitos e por enviar as mensagens de resposta sobre a decisão de autorização. O módulo de *Encapsulamento* é responsável por coletar as informações contidas nas requisições SAML que chegam e repassá-las ao controle de decisão no formato desejado. O módulo *Desencapsulamento* é responsável por formatar a decisão de autorização em um padrão SAML de mensagem de resposta desejada.

O módulo de *Recuperação de Políticas* agrupa as políticas necessárias requeridas pelo controle de decisão. O módulo de *Recuperação de Atributos* disponibiliza valores de atributos, que não estão presentes na requisição de autorização, necessários para recuperação de políticas envolvidas no processo de decisão. Finalmente o *Controle de Decisão* efetua a avaliação de políticas através do uso de algoritmos de avaliação, que geram a decisão de autorização sobre os direitos.

3.2. Modelo da Entidade de Criação, Distribuição e Gerenciamento de Licenças

A *Entidade de Criação, Distribuição e Gerenciamento de Licenças* (LCDME) é constituída pelos módulos *Rights Interpretation Module* (RIM), *License Creation Module* (LCM), *License Distribution and Storage Module* (LDSM), e *License Management Module* (LMM), conforme Figura 3.

O módulo RIM recebe a mensagem com a decisão de direitos, provinda da ARDE, interpreta a mensagem em formato SAML, extraindo os direitos contidos na mensagem e colocando-os em uma lista, enviada ao módulo LCM para criação de licenças. O módulo RIM também formata e envia as mensagens de requisição de direitos para a ARDE. O módulo LCM usa a linguagem XrML para criar as licenças digitais, com base na lista de direitos emitida pelo RIM. As informações de identificação do principal são enviadas pelo controlador no lado cliente, assim como as informações sobre o conteúdo. A licença é armazenada em um arquivo XML, e enviada ao módulo LDSM. No LCM, são implementados um processo interpretador de licenças e um processo de validação de condições, para verificar a integridade das licenças criadas. Estes processos de interpretação e validação também são implementados no controlador cliente e no LMM (para verificação de datas de expiração). O módulo LDSM executa as tarefas de distribuição da licença para o cliente, e armazenamento da licença numa base de dados XML, para controle e gerenciamento. As licenças são enviadas para o controlador no cliente, e o mesmo as armazena de forma segura na máquina cliente, e executa o gerenciamento de uso. O controlador envia mensagens periódicas para o LMM, com informações sobre o uso da licença.

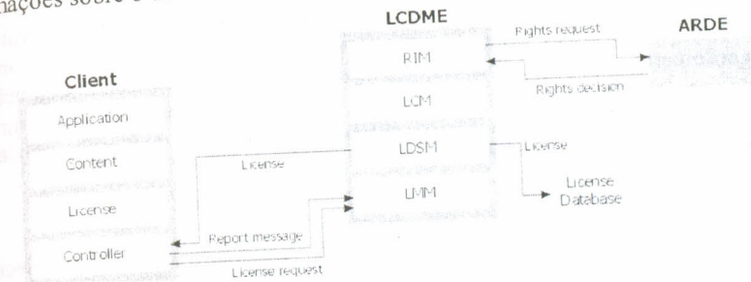

Figura 3. Módulos da LCDME.

O módulo LMM executa tarefas de gerenciamento de licenças no lado servidor, tais como verificar datas de expiração e enviar mensagens avisando ao cliente sobre a expiração da licença, além de verificar, a partir dos relatórios enviados pela aplicação controladora, se uma licença está sendo usada de modo indevido. O LMM também recebe os pedidos de licença da Entidade Cliente (a partir do controlador), e envia os pedidos para o RIM, que faz a formatação do pedido e envia a requisição em formato SAML para a ARDE. As licenças armazenadas na base de dados XML são excluídas quando expiram.

3.2.1. Implementação da Entidade LCDME

A implementação da LCDME é realizada com o uso da linguagem C++ para programação dos módulos. Também é utilizada a linguagem de especificação de direitos XrML para a criação de licenças, através do XrML SDK (*Software Development Kit*) [Wang et al. 2002], fornecido pela *ContentGuard*, empresa criadora e desenvolvedora da linguagem XrML. A linguagem XrML foi escolhida por ser uma tecnologia baseada em XML e por ser bem aceita no mercado, sendo utilizada por vários desenvolvedores de aplicações DRM, como a *Microsoft*. O *parser* utilizado foi MSXML 4.0, da *Microsoft*. Os processos de interpretação de licenças e validação de condições foram desenvolvidos com base nos exemplos do XrML SDK. O *parser* XML usado no módulo LCDME foi o MSXML 4.0, da *Microsoft*. Também é configurado o *Microsoft Platform* SDK, necessário para desenvolvimento de aplicações para *Windows*.

4. Conclusões

Este artigo propôs uma arquitetura para distribuição de direitos de acesso digitais, unindo aspectos do controle de acesso tradicional e aspectos de DRM que realizam o controle de uso do conteúdo.

No que diz respeito ao controle de acesso tradicional, a arquitetura proposta definiu um modelo para ARDE que pode utilizar políticas de segurança para estabelecer direitos de acesso ao conteúdo protegido, através do uso de uma linguagem padrão de definição de política, a XACML. Quanto ao controle de uso, a arquitetura DCDMA usou ainda outra tecnologia baseada em XML para especificação de licenças digitais (XrML), que possibilita o controle de uso depois da distribuição do conteúdo. Diferente dos trabalhos analisados na literatura, a arquitetura proposta proporciona o controle de uso de licenças também no lado do servidor dificultando o uso inadequado das licenças.

A DCDMA promoveu a interação entre os componentes do controle de acesso e

os componentes de controle de uso utilizando padrão SAML e incorporando aspectos de segurança que são inexistentes na literatura relacionada. O desenvolvimento do protótipo contribuiu para refinar alguns aspectos importantes da arquitetura, atuando diretamente na interligação entre o controle de acesso tradicional e o controle de uso. A definição de padrões de segurança e comunicação específicos para DRM , como trabalhos futuros, é de grande importância, na medida que sistemas operacionais modernos tendem a implementar esse tipo de controle de acesso.

Referências Bibliográficas

Chong, J.C.N., Buuren, R.V., Hartel, P.H. and Kleinhuis, G. (2002) "Security Attributes Based Digital Rights Management", In: Joint International Workshop on Interactive Distributed Multimedia Systems/Protocols for Multimedia Systems (IDMS/PROMS), Portugal, November, 18 p.

Erickson, J.S., Williamson, M., Reynolds, D., Vora, P. and Rodgers, P. (2001) "Principles for Standardization and Interoperability in Web-based Digital Rights Management", In: W3C Workshop on Digital Rights Management, France, January.

Godik, S. and Moses T. "eXtensible Access Control Markup Language (XACML) Version 1.0". OASIS Standard, 18 February 2003.

Ianella, R. (2001) "Open Digital Rights Management", In: W3C Workshop on Digital Rights Management, France, January, 5 p.

Maler, E., Mishra P., Philpott, R. "Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1", OASIS Standard, 18 July 2003.

Park, J., Sandhu, R. and Schifalacqua, J. (2000) "Security Architectures for Controlled Digital Information Dissemination", In: 16th Annual Computer Security Application Conference, USA, December, p. 224-233.

Park, J. and Sandhu, R. (2002) "Originator Control in Usage Control", In: 3rd International Workshop on Policies for Distributed Systems and Networks, USA, June, p. 60-66.

Rosenblatt, B., Trippe, B. and Mooney, S. (2002) "Digital Rights Management – Business and Technology", M&T Books, 1st Edition, USA, 288 p.

Sun Microsystems, Inc. "Sun's XACML Implementation". 2003-2004. Disponível em http://sunxacml.sourceforge.net/javadoc/index.html .

The Ohio State University Corporation for Advanced Internet Development. "The OpenSAML version 1". 2002. Disponível em

http://wayf.internet2.edu/opensaml/java/doc/api/index.html.

Vollbrecht, J. et al. "AAA Authorization Framework". The Internet Society, RFC-2904, August 2000.

Wang, X., Lao, G., DeMartini, T., Reddy, H., Nguyen, M. and Valenzuela, E. (2002) "XrML – eXtensible rights Markup Language", In: ACM Workshop on XML Security, USA, November, p. 71-79.