


Microsoft
Windows Server 2003

Microsoft Rights Management Solutions for the Enterprise: Persistent Policy Expression and Enforcement for Digital Information

Microsoft Corporation

Published: February 20, 2003

Abstract

One of the touchstones of Trustworthy Computing is the availability of technology that can reliably protect content and keep digital information private. The dramatic rise in cybercrime and the emergence of related new legislative requirements point to the need for better means to protect digital information. While the information technology solutions currently used by organizations such as financial institutions, government agencies, healthcare organizations and professional services firms address many concerns adequately, once enterprise information is transported beyond the firewall, the perimeter-based methods typically used for protecting information cannot enforce persistent business rules regarding its use and distribution.

This paper discusses the Microsoft® Windows® Rights Management Services for Windows Server 2003 and related technologies. Windows Rights Management provides easy-to-use, flexible and ongoing policy expression and enforcement to help enterprise customers control and protect digital information, including proprietary business information and other vital enterprise resources.

This is a preliminary document and may be changed substantially prior to final commercial release of the software described herein.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2003 Microsoft Corporation. All rights reserved.

Active Directory, Microsoft, Microsoft, the Windows logo, Windows, Windows Media, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Contents

Introduction: Safeguarding Digital Information in an Increasingly Connected World.....	1
Why Current Solutions Cannot Address This Growing Problem	1
Expanding Rights Management in the Windows Platform.....	3
Windows Rights Management Components.....	5
The Rights Management Workflow	6
• Creation and policy expression	6
• Distribution and licensing	6
• Consumption and policy enforcement.....	6
The Benefits of Windows Rights Management.....	7
Ease of Use and Flexible Control.....	8
Maintaining Existing Investments.....	9
Summary	10
Appendix The Emerging Standard for RM Interoperability.....	11
How XrML Works	11
Related Links	12

Introduction: Safeguarding Digital Information in an Increasingly Connected World

Loss of confidential information is causing significant damage to enterprises. Reporting in January 2003 on the “exponential” increase in computer-related crimes, The New York Times cited “a tightening economy, the increasing riches flowing through cyberspace and the relative ease of such crimes” as some of the reasons computer-savvy outsiders as well as corporate employees make off with confidential information. Worldwide, losses due to cybercrime (crime related to computers, technology and the Internet), are estimated in the millions or even billions of dollars a year.¹

All digital information is susceptible to attack. That includes everything from confidential meeting notes and customer-facing online content to military defense strategies and other classified government information. Last year PricewaterhouseCoopers reported that nearly a third of the most serious security breaches in recent years were due to insiders; and in large companies, the number jumped to nearly half.²

In addition to the threat of computer-related crime, the finance, government, healthcare and legal sectors are increasingly challenged by the need to tighten protections for digital information to comply with emerging legislative standards. The Healthcare Insurance Portability and Accessibility Act (HIPAA³) and the Gramm-Leach-Bliley Act (GLBA⁴) in the financial services industry are some relatively recent legislative measures that require enterprises to take specific steps to protect digital information.

Why Current Solutions Cannot Address This Growing Problem

The information technology industry has worked diligently to keep up with the increasing need to safeguard digital information. Network access can be limited with firewalls; access to certain digital information can be restricted with access control lists (ACLs). Such technologies meet important needs. Strategies that rely solely on such perimeter-based methods resemble an egg: If the network “shell” is cracked, digital information could be exposed. If someone does gain access to the network, there is currently no additional layer of protection.

Public key infrastructures (PKI) using S/MIME encryption are a valuable and widely used means to help keep enterprise e-mail secure while in transit or help ensure that it is first opened by the right person. However, recipients are still free to do whatever they want with any information that falls into their hands. For example, it could be forwarded to another person, copied to another computer or posted online. Even accidental security breaches can cause serious harm to an enterprise. Sensitive e-mail or documents could be forwarded mistakenly to a recipient with potentially malicious intent.

¹ “Crime Is Soaring in Cyberspace,” New York Times, Jan. 27, 2003, online edition.

² Information Security Breaches Survey 2002, PWC (PricewaterhouseCoopers).

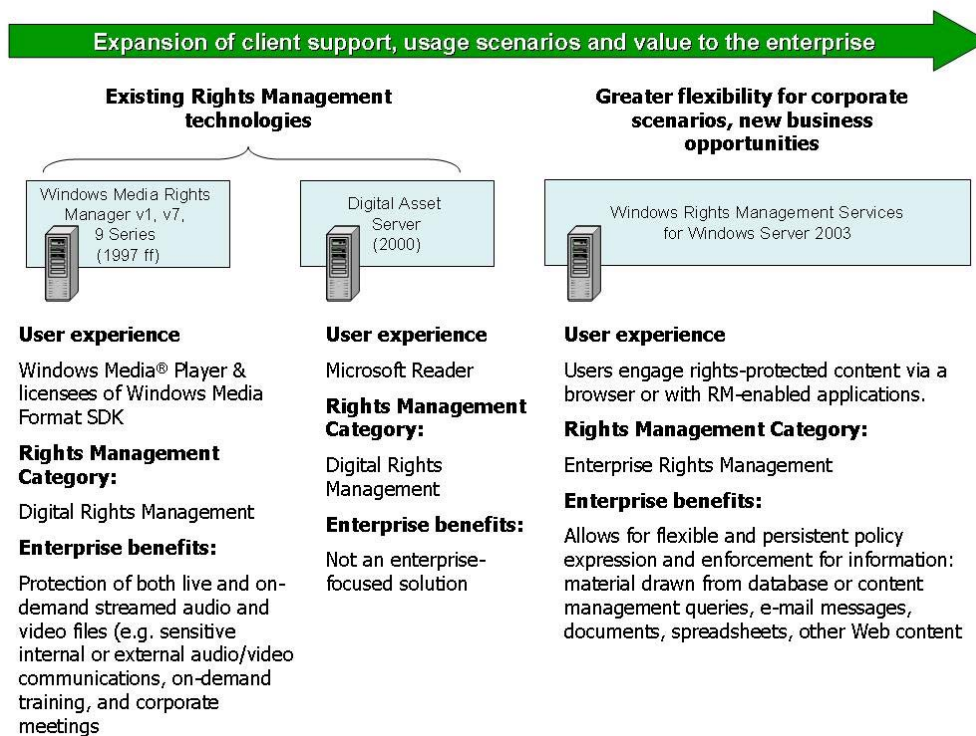
³ Passed in 1996, HIPAA relates to healthcare coverage and, for example, how companies may use medical information.

⁴ Gramm-Leach-Bliley, also known as the Financial Services Modernization Act, was passed in 1999.

In many cases, information is at risk within the firewall perimeter once employees transport that information from corporate servers to their own desktops, or when it is saved to some form of removable media such as CD-ROM. The risk is magnified once employees transport information beyond the corporate firewall. The perimeter-based solutions currently in use are unable to help enforce business rules regarding the use and distribution of digital information. Instead, enterprises need an end-to-end software solution to help safeguard information doggedly.

Expanding Rights Management in the Windows Platform

Successful companies depend more and more on integration with customers, partners, suppliers and regulatory agencies. As a result of this integration, Microsoft Corp. has heard from customers that they need new ways to control how their digital information is consumed and used. Rights Management Services (RMS) has been developed in response to that need, and combines Windows® Server 2003 features, developer tools, and tested and proven security technologies, including encryption, certificates and authentication. This new technology will soon be available to help protect enterprise information such as merger and acquisition plans, loan applications, payroll and salary information, and production status reports, including the growing amount of such information that is available on enterprise



information portals.⁵

Figure 1. Windows Rights Management technologies extend digital information protection beyond traditional media uses to help protect enterprise information and enforce written corporate policies.

Easy to use, flexible and persistent, Rights Management (RM) helps customers control and protect digital information both online and offline, inside and outside the perimeter of the firewall. Using RM represents an opportunity to help protect and enhance all types of digital information within intranet and

⁵ "... the rapid rate of EIP software adoption will create a \$1 billion opportunity by 2003, and the market will continue to grow to \$2.4 billion in 2005," IDC Bulletin #25087, July 2001.

some extranet scenarios. For example, RM can help protect information in a wide range of situations, including the following:

- **Intranet content.** A manager with a large multinational pharmaceuticals company has been granted access to the online sales system. She navigates to the year-over-year sales information on the enterprise information portal, and the information is displayed on-screen within her browser. Because the information is sensitive, specific usage restrictions have been applied to the report she sees: The manager gets the information she needs, conveniently, but because she cannot print, copy or paste the information on screen, the company's sensitive sales data are protected from inadvertent or deliberate sharing with a close competitor.
- **E-mail communications.** A senior partner in a law firm needs to send e-mail to his partners with a confidential contract proposal attached. In his word processing client, he specifies that only senior managers may read the proposal, and that, in line with their policies regarding confidentiality, they may not copy, paste or edit the information. As a further precaution, the partner specifies that the e-mail itself can not be forwarded. The recipients receive the mail, and their e-mail and word processing clients transparently enforce these policies and secure the appropriate permissions so they can view the proposal. All partners are confident that the proposal will not be seen by those unauthorized to view it, and the firm worries less about information leaks, which may damage the ongoing negotiations.
- **Documents.** Using a simple on-screen dialog prompt built into her word processor, a worker at an advertising agency applies RM to the latest, not-yet-released print advertising copy to allow the client to view and edit the file for one week. She sends the rights-managed document to multiple employees at the client company via e-mail. When each of the client employees downloads the document, his word processor enforces the time-limited rights; after a week, he can no longer open the document. To keep new product details related to the advertising campaign in the right hands, the agency representative tracks the comments from various client employees using a spreadsheet that is also protected with Rights Management.

Because RM policy expressions can remain with information — even in transit — rather than residing on a corporate network, the policies can be enforced even when the rights-managed information leaves the network. By providing the means to manage how information is used and distributed no matter where it goes, RM technologies help enterprise customers realize more of the potential of working with computers. (The various RM policies that can be applied to information are discussed in the section “The Benefits of Windows Rights Management.”)

Windows Rights Management Components

Rights Management combines Microsoft Windows Server 2003 features and developer tools. The components necessary for end-to-end information protection are server or client mechanisms and deliver either core RM functions or the tools needed to use or extend them. (To provide benefit, RM components must be in place at all three levels of the digital content workflow described under “The Rights Management Workflow.”)

Inside the Enterprise Firewall

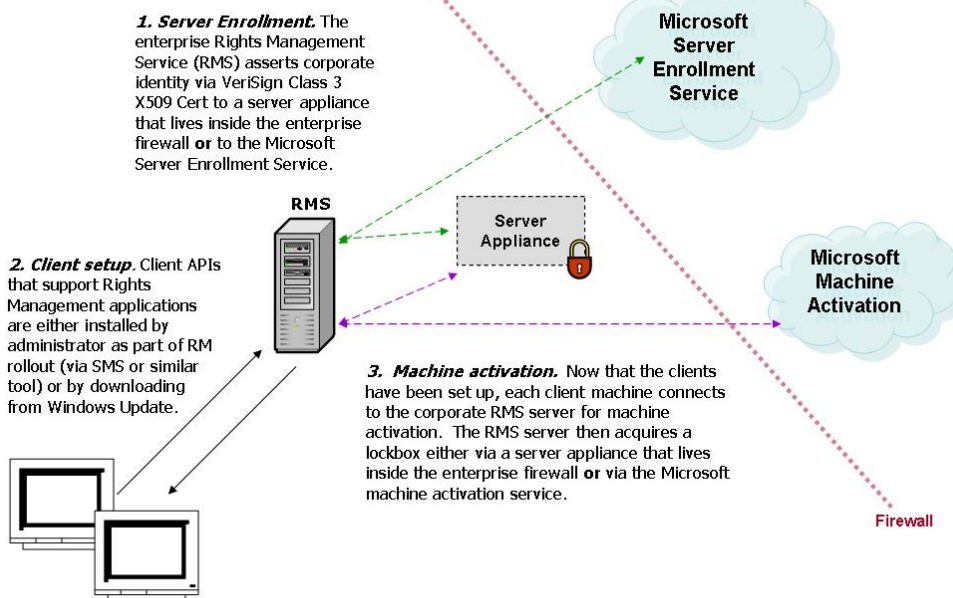


Figure 2. Deployment of Windows Rights Management within the enterprise

On the server side, Windows Rights Management Services on Windows Server 2003 handles the core licensing, machine activation, enrollment and administrative functions. An RMS software development kit (SDK) and application programming interface (API) will provide information such as sample code and documentation so independent software vendors (ISVs), systems integrators (SIs) and corporate developers can work with the core RM functions and extend core functionality.

For client applications, the Rights Management client API will be available for Windows clients (Windows 98 Second Edition and later). In addition, the RMS client SDK includes tools and documentation to help ISVs, SIs, corporate developers and others extend their solutions by incorporating RM on the desktop. With these tools, professionals can build “trusted client” applications: programs able to create, distribute, and consume rights-managed content.

For added protection and interoperability, Rights Management uses the Extensible Rights Markup Language (XrML), an emerging rights expression language (REL) standard based on XML. XrML offers a common, simple-to-use means for expressing and managing rights and policies for digital content and

services. It is a flexible, extensible and interoperable standard equipped to meet any organization's needs, regardless of industry, platform, format, media type, business model or delivery architecture. (More information about XrML can be found in the appendix.)

The Rights Management Workflow

Along with technology, people and processes are key ingredients in any security mix. By using tested and proven security technologies, including encryption, digital certificates and authentication, Windows Rights Management gives enterprises the means to implement processes that empower people to protect enterprise information better.

Rights Management protection is designed to be easy to use and transparent to end users. To protect digital information with RM technologies, information workers simply follow the same logical and fundamentally interlinked workflow they already use with digital information.

- Creation and policy expression.** With RM-enabled applications, users can easily create rights-managed information. The content management and authoring applications that people use every day — for example, computer-aided design (CAD) applications or Microsoft Office — can incorporate RM functionality. Using common task management procedures within a familiar on-screen environment, users can assign policies to any digital object, such as an e-mail message or document. Custom-built templates can be used to apply predefined Rights Management policies automatically. Via RMS, line-of-business applications can manage creation and policy expression automatically, integrated into an existing enterprise workflow.
- Distribution and licensing.** Windows Rights Management Services operates at the core of the protected digital content flow. RMS is used by creation and policy expression applications and consumption and policy enforcement applications to issue a license to a user based on the expressed policies and the user's identity. In this way, for example, a consulting firm can apply RM to an industry report so, when distributed, it cannot be opened except by a paying customer.
- Consumption and policy enforcement.** Consumption and policy enforcement applications, or trusted clients, are computer systems or applications such as a custom payroll application or a word processor designed for use with RM technologies. A trusted client, using the RM client API in Windows 98 SE or later to communicate with RMS, requests a license for protected information and enforces the rights expressed in the license to allow viewing and consumption of the digital information as defined by the content owner in the publishing license. Other examples of trusted clients include Microsoft Office, a Rights Management Add-on for Internet Explorer, or any other RM-aware application.

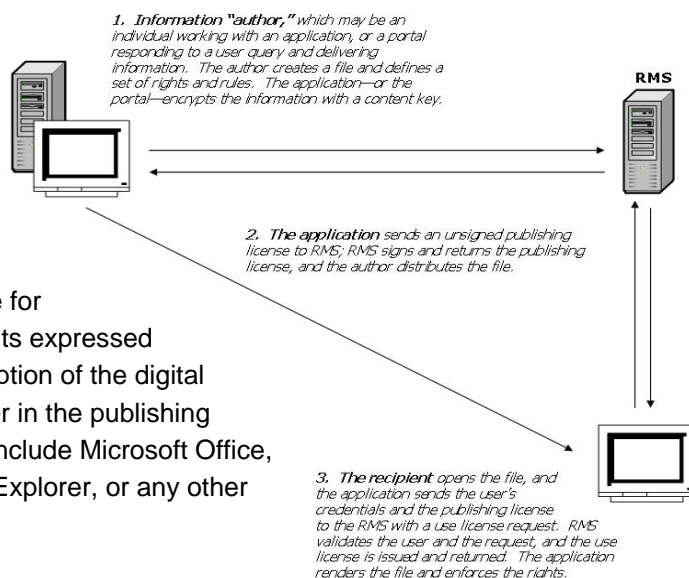


Figure 3. The Windows Rights Management workflow

The Benefits of Windows Rights Management

Windows Rights Management adds value to any organization’s security mix by providing enterprise users with a flexible, easy way to control most of the types of digital information they typically create and use. For online information (such as database-backed dynamic content data on benefits and payroll intranet sites or enterprise information portals), as well as e-mail communications and documents, RMS can help enforce policies such as restricting the ability to print, forward and edit data. Permissions can be set to expire at a specific point, such as a number of days after publishing or at regular intervals, requiring acquisition of a new license. In addition, enterprise policies can be enforced and centrally managed: Templates for policies such as “company confidential” or “attorney-client privilege” are easy to create and deploy.

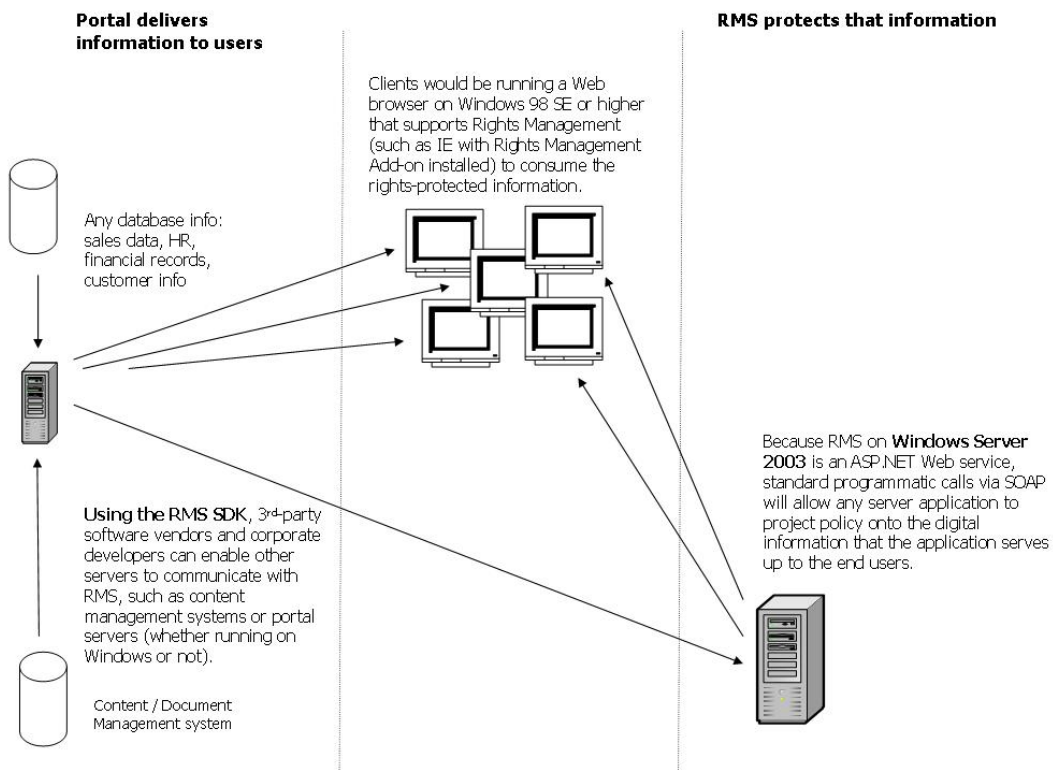


Figure 4. Among other uses, RM technologies can help enforce policies for the use and distribution of the dynamic, database-backed content frequently available on enterprise information portals.

With these abilities, government agencies, private consulting firms, healthcare organizations, stockbrokers and other enterprises gain effective means to help safeguard digital information such as the following:

- **Operations.** Quality control statistics, deployment plans and proposals, inventory data, benchmarking studies, production details, purchase orders, shipping reports and enterprise resource planning data
- **Finance.** Merger and acquisition plans, contract bidding plans and proposals, financial performance statistics, insurance claims and loan applications, cost forecasts, budgets, invoices, expense reports and contracts
- **Personnel and human relations.** Information about recruiting, payroll and salary; medical records; employee and supplier performance analyses; and organizational announcements
- **Research and development.** Project specifications and product overviews, white papers and official research reports, business development strategies, supplier information, cost-benefit analyses, production status reports, documentation and training manuals
- **Marketing and public relations.** Information about pricing and promotions, drafts of brochures and newsletters, presentations, press releases, testimonials, sales reports and analyses, business plans, customer and constituent requirements and feedback

Ease of Use and Flexible Control

Centralized administration, auditing support, adaptable usage policy, and revocation and exclusion support help enterprises gain better control over their digital information. RM-enabled software can help enforce company policies that have been rendered as centralized templates (such as “company confidential”). Administrators can centrally manage trust relationships via control of RM credential issuance or revocation and exclusion policies. Managers can review comprehensive, internal logging records to monitor licensing activity, including requests granted or denied.

Rights Management also offers flexible deployment options, from single-box deployments to global distributed topology, and provides the tools needed to deploy and use RM in a wide variety of scenarios. In-house and other developers can build Rights Management into custom applications and systems by using RM software development kits. In addition, RMS can easily scale up or out as needed and meet the needs of high-availability networks. Broad client support, centralized Web-based administration, published RM client and server APIs, and Windows Active Directory® integration work together to help make RM flexible.

Perhaps most important, Rights Management is easy to use. Software developers have many options when implementing Rights Management technology into their applications. Based on these options, the ability for recipients to print, copy and edit information can be granted singly or in any combination, and can be customized for a specific piece of information as the application permits. Windows Rights Management delivers an extensive, scalable foundation for building Rights Management into an

application. This puts the power in the hands of the application developer, so applications can present RM policy enforcement mechanisms that are consistent with the user interface of the application. Rights-managed information can be created and worked with entirely offline. Protected information can be accessed and used on multiple machines. To work with rights-managed data, users simply click to open it. Key and license management and the other technical considerations that help keep information safe are designed, for the most part, to be transparent to end users.

Maintaining Existing Investments

Windows Rights Management is designed to make the most of existing infrastructure investments. Rights Management Services uses Active Directory for service discovery and Windows NT® LAN Manager (NTLM) authentication. With the flexibility of Windows authentication, RMS can utilize smart card and biometric devices as well as other alternate authentication methods supported by Windows.

The Windows Rights Management client SDK will be available to developers and ISVs to add RM functionality to their programs so, in addition to Microsoft applications, non-Microsoft applications may incorporate RM to help protect digital information. The resulting availability of enhanced Rights Management capabilities for both Microsoft and non-Microsoft applications enables diverse, multi-tiered solutions.

For recipients of RM-protected content who do not have a program that uses RMS, the Rights Management Add-on for Internet Explorer, scheduled to be available for download in 2003, will add RM features to the browser so Windows can be used to view rights-managed documents including e-mail and other HTML information that is protected. The Rights Management Add-on will enable broad intranet and Internet portal scenarios by presenting rights-protected HTML to clients.

For government agencies and others that maintain and operate customized internal programs, the RM client SDK provides the technology needed to help express, manage and enforce information security policies.

Summary

More and more, enterprise success depends on the ability to protect and control information. Windows Rights Management provides flexible, easy-to-use tools to help people do that. Designed to make the most of existing infrastructure investments and to integrate easily with existing Microsoft applications and other technology solutions, RM fosters a new level of assurance that digital information can be protected at the file level against negligence and crime.

Appendix The Emerging Standard for RM Interoperability

Microsoft is a strong believer in the benefits of industry standards and well-documented technical specifications, such as HTTP, TCP/IP and XML, which have been tested and reviewed by a standards organization. Industry standards must show technical competency. Therefore, standards organizations, such as the World Wide Web Consortium (W3C) and Moving Picture Experts Group (MPEG), review proposed standards to ensure that their developers have followed correct guidelines. In addition, standards organizations test proposed standards in numerous independent and networked scenarios.

Voluntary adherence to a standard rights expression language will develop critical rights management interoperability benefits that are currently latent. The emerging standard, XrML — which has been recognized by MPEG — offers many innate interoperability benefits. XrML provides digital properties with a simple-to-use, universal method for expressing rights linked to the use and protection of digital information, including Web services. Developers can integrate new and existing rights management systems easily with XrML. Moreover, XrML is currently the only rights expression language used in working rights management solutions. Microsoft, which has employed XrML since its inception, looks forward to the many important benefits that rights management interoperability (based on the XrML standard) will bring to bear.

How XrML Works

XrML specifies a rights expression language that trusted systems within a trusted environment can use to express digital information policies. XrML licenses can be applied to trusted information in any format, such as e-mail, office productivity tools, database contents, e-commerce downloads, line-of-business programs and customer relationship management systems, to name a few. XrML licenses can then be enforced through any trusted rights management system that uses the XrML standard.

The rights to be managed are expressed in an XrML issuance license attached to the file. The issuance license is an expression of how the information owner wants it to be used, protected and distributed. The issuance license and the user's identity are passed to the rights management system, which builds a license.

These licenses are easily interpreted and managed by various interoperable rights management systems because they all use the XrML standard. Managing information online using licenses provides ease of access from any location. After the license is downloaded, the rights management is effective both online and offline because the rights persist with the file wherever it goes.

XrML supports an extensive list of rights, and applications can define additional rights to meet particular needs, which helps to ensure that enterprises can build many business, usage and workflow models to meet their specific requirements.

More information about XrML can be found at their [Web site](http://www.xrml.org/) at <http://www.xrml.org/>.

Related Links

- Those with questions about Windows Rights Management can send e-mail to rm_info@microsoft.com.
- Additional information about Microsoft products and security is readily available online at <http://microsoft.com/security/>.
- Details about Microsoft products and privacy can be found at <http://microsoft.com/privacy/>.
- More information about the Trustworthy Computing initiative can be found online at <http://www.microsoft.com/presspass/features/2003/jan03/01-15twcanniversary.asp>.