The Digital Property Rights Language

Manual and Tutorial - XML Edition

Version 2.00 — November 13, 1998

LIMITED DISTRIBUTION - REVIEW PURPOSES ONLY

The material contained in this document is provided for review purposes only. Receipt of this document does not constitute a license, actual or implied, to any intellectual property contained herein. All material contained in this document is the intellectual property of the Xerox Corporation.

-

1. INTRODUCTION

The *Digital Property Rights Language Manual* is a work in progress specifying a language for describing rights, conditions, and fees for using digital works. The Digital Property Rights Language (DPRL) is intended to support commerce in digital works, that is, publishing and selling electronic books, digital movies, digital music, interactive games, computer software and other creations distributed in digital form. It is also intended to support specification of access and use controls for secure digital documents in cases where financial exchange is not part of the terms of use.

This manual is being circulated for review among publishers, platform vendors, authors, librarians, and others interested in the issues involving rights and fees for digital works. Our purpose in circulating the manual is to solicit feedback and suggestions that can guide us in developing the language and establishing appropriate standards. The use of a standard language for usage rights on digital property ensures that trusted systems can exchange digital works and interoperate. The trusted systems are for authoring, playing, and selling digital works. They include personal systems, on-line storefront systems, library systems, and others.

The digital property rights language describes distinct categories of uses for digital works in terms of "rights," including rights to copy a digital work, or to print it out, or to loan it, or to use portions of it in derivative works. DPRL also describes conditions and fees (if any) relevant to such uses.

Before describing the language itself, this introduction first discusses the commercial context for DPRL. It discusses the intended audience for this manual and how usage rights would actually appear to creators, publishers, and consumers of digital works. Finally, it describes our design goals and assumptions for the language.

For variety in expression, we use the words digital property rights, digital rights, and usage rights synonymously. Similarly, we use the words digital property rights language, digital property language, digital rights language, and rights language synonymously. We also use the terms digital publications, digital documents, and digital works synonymously.

1.1 Enabling Commerce in Digital Property

Digital technology has shifted the balance of practice in the social contract between those who create and distribute works and those who use them. For many kinds of digital works, it is very easy to use and duplicate a work without having authorization or providing compensation. With electronic networks, it is easy to distribute unauthorized copies of a digital work to points around the world, without knowledge of the publisher or author.

For some publishers, the issue of unauthorized distribution represents too great a business risk and they do not publish in digital form. For others the revenue losses are affordable, but they lead to billing and distribution schemes that are cumbersome. For example, distributors of digital works typically bill all users the same amount regardless of the use to which the consumers will put the work. Some digital publishers rely on the honesty of users not to replicate a work or use it in unauthorized ways after an initial purchase. Ironically, some publishers figure that some "leakage" of works that need periodic upgrading (such as computer software) helps to increase their installed base. However, even for computer software, it is often reported that there are more unauthorized copies in use than authorized ones.

Consumers of digital works are also poorly served. It requires much more time, effort and money to be honest than to slip beyond the legal rights for use of a digital work. Consumers sometimes view the creators of a work as opponents, and try to "get away with" unpaid use because they have paid so much for other works. Given the lack of safeguards and reliable billing services, few publishers have been willing to distribute their works digitally over computer networks. Consequently, consumers miss out on the convenience of 24-hour software shopping and on-line delivery. Since there are no reliable and general means for determining how much software is used, users must usually pay the same for software regardless of how much use they make of it.

Various approaches have been proposed to create a commercially viable means of distribution. These approaches are based on concepts such as trusted systems, semi-trusted systems, digital envelopes, and secure containers. The most general approaches are based on two simple ideas: that digital works can be bought and sold among trusted systems and that works have attached usage rights that specify what can be done with them and what it costs to exercise the rights.

Different publishing and distribution systems require different kinds of subsystems and capabilities. The digital property language is primarily concerned with those systems that are directly involved in buying, selling, and using digital works. These systems would generally be implemented as trusted systems.

A trusted system is a system that can hold digital works and which can be trusted to honor the rights, conditions, and fees specified for a work. Trusted systems can take different forms, such as "trusted players" that play digital works, or "trusted readers" for reading digital works or "trusted servers" that may provide access to digital works on a network. Recognizing that different applications require different kinds of trusted systems and different levels of security, we use the terms trusted system and repository interchangeably to refer generically to systems relied on to keep documents secure and to honor usage rights

Different implementations of trusted systems have different requirements for security and different approaches. In the most secure approaches, all of the hardware and software on the platform is certified to honor digital rights. Other approaches focus on the use of so-called secure envelopes or containers, emphasizing transmission and storage of information. All such approaches have *some* elements that are assumed to be trusted and which can be circumscribed by boundaries of trust. These boundaries may be the boundaries of program code assumed not to be altered, data files assumed not to be acessible, language interpreters (such as Java) assumed to follow certain rules, or physical hardware assumed not to be compromised. The security of a trusted system depends in large measure on its vulnerability across these boundaries. For the purposes of this document, we use the term "trusted system" in a generic sense to refer to all systems for security and commerce in digital works, regardless of the techniques used to create a basis for trust.

We use the term "semi-trusted system" to refer to a class of repositories that have two levels of storage - regular storage and trusted storage. Regular storage is file space accessible to untrusted programs. Generally, this is used to hold encrypted works. Trusted storage is special storage not readily accessible to untrusted programs. Trusted storage is for encryption keys, billing data, some non-transferable digital certificates, and digital tickets.

Beyond trusted systems are several other kinds of systems, made up of hardware, software, and communications elements. For example, trusted systems would confirm credit and exchange billing data with financial clearing houses. In contrast to "authoring systems," we use the term "digital publishing systems" to refer to systems that can import digital works in native formats, interact with a publisher or distributor to add usage right information, and export the digital works in encrypted forms or in digital containers. We use the term "network sales server" to refer to systems that offer documents for sale on-line, such as on the World Wide Web.

1.2 Scope of this Document

This document explains the basic concepts for managing digital works in trusted systems, describes the language syntax and semantics, and provides examples of typical specifications of usage rights. It does not provide specifications for security in trusted systems, propose specific applications, or describe the details of the accounting systems required.

One of the goals of our work in usage rights is to develop an approach and language that can be used throughout the publishing industries and in other industries as well. This paper does not address the agreements, coordination or institutional challenges involved in achieving that goal. See (Stefik, 1995) for a sketch of some of the institutional challenges.

1.3 Basics of Digital Property Rights

Digital property rights (or "usage rights" for short) are rights associated with digital works and their parts that describe how the works can be used. Here are some basic concepts:

- Rights are associated with parts of a digital work (and with folders).
- Every class of usage right has a corresponding transaction.
- The transaction defines what a repository does when the right is exercised.
- Rights are described in sentences of a machine-interpreted language having a grammar.
- The transactions for a given work are parameterized by the information in the usage rights sentences for the work.
- The rights on a work can be changed later, if the change is authorized by the rights owner.

1.4 Interfaces to Digital Property Rights Specifications

Specifications in the digital property language are established by creators of digital works and also by publishers and distributors. Specifications are used by consumers as they select and use digital works. However, creators, publishers, distributors, or consumers would seldom (if ever) look directly at specifications written in the language.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | sales@docketalarm.com | 1-866-77-FASTCASE

fastcase®
Smarter legal research.