Executive Summary

“DRM technology must ensure the security, privacy, neutrality, commercial reliability and trusted interoperability of those applications and services which protect and manage rights in connection with all forms of digital information, and we must, in our development of this technology, be guided by the principle of maintaining a free and effective commercial society that equitably and in a balanced fashion supports and safeguards the rights of all participants.” – Adapted from [86]

The main aim of the research behind this thesis was to investigate and develop a distributed digital rights management (DRM) model that manages access to and use of digital information objects persistently and fine-grainedly, and protects the privacy of users in a flexible and secure fashion. In order to do this, this model would necessarily comprise techniques, frameworks, processes, procedures and algorithms for the management of rights, and balance the privileges and responsibilities of rights-holders against the permissions and obligations of rights-users in a fair, equitable, and mutually rewarding manner, making all stakeholders winners.

DRM is a complex and multifaceted concept which is affected by many disciplines which it, in turn affects. This thesis first investigates what kind of multidisciplinary DRM framework is needed to give a holistic view and understanding of DRM which is a necessary basis for the identification and examination of the factors forming a necessary prerequisite for the establishment of trust and confidence in DRM. It then proposes a suitable integrated framework and describes it. The successful application of the proposed framework to a specific domain, e-government, is then described. The domain of e-government is a good testing ground since in e-government the correct handling of privacy, security and trust is indispensable if it is to function and be accepted by citizens. The
necessary basis for any fungible DRM framework is technology, technology which is reliable and trusted, so that it enables bona fide users to generate, distribute, store and use digital information objects securely and confidently. Consequently, the examination of DRM technology and its application forms the core of this thesis, which describes a distributed DRM model (successfully developed and implemented in the course of the research this thesis is based on) based on six trust-building blocks. Two of these trust-building blocks are described in detail. The first is the core rights enforcement services (authentication, authorization, and privacy protection) that are responsible for the actual fine-grained control of access to and usage of digital information objects and the protection of users’ privacy. The second is the rights-carrying and self-enforcing object that carries with it access and usage rights which it itself enforces, preserving the confidentiality and integrity of its encapsulated digital information content.

The results presented in this thesis show that providers can assert their authority over digital information objects and prevent (or at least deter) the illegal copying, forgery, and distribution of them, and consumers (in this case consumer communities like schools) can protect their privacy while availing themselves of the rights of access and usage granted to them by providers and handle correctly intellectual property rights to their own digital information objects. The specification of rights and requirements can be made by both providers and consumers, and the responsibility for their enforcement can be shared between them.