

# **Adopting Digital Rights Management Systems: An Institutional Perspective**

**Claudio Huyskens**

**Claudia Loebbecke**

**Petar Djekic**

Department for Media Management

University of Cologne

Pohligstr. 1, 50969 Koeln, Germany

Tel. +49-221-470-5364, Fax: -5300

{claudio.huyskens|claudia.loebbecke|petar.djekic}@uni-koeln.de

As business processes continue to be transformed into the virtual real, organizations face a growing body of information and knowledge embodied in digital files. However, this has caused problems for organizations in terms of information security and integrity. Security points to only authorized access. Integrity refers to the protection of digital files from corruption or illegitimate modification. Due to the ubiquity of network connections, digital files have become increasingly prone to security and integrity attacks. This is well documented by daily headlines on theft of credit card information and infringement of intellectual property rights.

To protect digital files and the information embodied, organizations rely on Digital Rights Management Systems (DRMS). These are information systems that persistently enable description, identification, protection and tracking of different digital rights across operating systems and media. Digital rights refer here to the set of access and usage rules particular to one or more digital file(s). Digital rights management (DRM) describes the management of such digital rights.

Current DRM research focuses on the consumer experience of DRMS and issues in DRMS architecture (e.g., Felten, 2003; Iannella, 2001; Jackson, Singh, Waycott, & Beekhuyzen, 2005; Kwok, Yang, Tam, & Wong, 2004; Mulligan, Han, & Burstein, 2003; Safavi-Naini, Nicholas, & Uehara, 2004). However, DRM research has paid little attention to adoption and acceptance of DRMS from an organizational perspective. By adopting a DRMS, organizations may increase security and integrity of digital files and of the information and knowledge embodied in them (e.g., patents and algorithms).

Based on the research on adoption of intra-organizational information systems (e.g., Chwelos, Benbasat, & Dexter, 2001; Zhu, Kenneth, & Xu, 2003), this paper investigates which issues may facilitate or inhibit an organization's intention to adopt a DRMS.

We consider three contexts: the technological, organizational and environmental context. The technological context points to structural properties of technologies already present within the organization, such as the homogeneity and connectivity of the IT infrastructure. The organizational context considers the organizational members' IT skills and the management support for DRMS adoption. Socio-cultural issues such as the organizational culture play a stronger role, since DRMS can affect the core processes of how organizational members manage and utilize digital files. Finally, the environmental context reflects the field an organization operates in and how it influences the adoption decisions. For example, an organization may be obliged to adopt a DRMS by legislative regulations such as the Sarbanes-Oxley-Act, which imposes specific requirements regarding audit trails and protection from document tampering. California's Resident Information Protection Laws are

another example, which requires organizations dealing with personal information, e.g., financial account numbers, to ensure the security of such information. If an organization faces strong competition, it may want to adopt DRMS in order to gain a competitive advantage (Porter & Millar, 1985; Premkumar, Ramamurthy, & Crum, 1997). This advantage could result from a reduced leakage of information to organization outsiders and hence impede competitors to develop competitive products ahead of time.

Overall, the increase in digital files due to ongoing digitization and connectivity of information systems raises the need for DRMS and hence for research on issues dealing with DRMS adoption by organizations. This paper provides first insights into our study of DRMS adoption, which is based on semi-structured interviews of senior informed managers from various organizations.

## References

- Chwelos, P., Benbasat, I., Dexter, A. S. (2001) Research Report: Empirical Test of an EDI Adoption Model, *Information Systems Research*, 12(3), 304-322.
- Felten, E. W. (2003) A Skeptical View of DRM and Fair Use, *Communications of the ACM*, 46(4), 57-59.
- Iannella, R. (2001) Digital Rights Management (DRM) Architectures, *D-Lib Magazine*, 7(6).
- Jackson, M., Singh, S., Waycott, J., Beekhuyzen, J. (2005) DRMs, Fair Use and Users' Experience of Sharing Music. Paper presented at the Proceedings of the 5th ACM Workshop on Digital Rights Management, Alexandria, VA, USA.
- Kwok, S. H., Yang, C. C., Tam, K. Y., Wong, J. S. W. (2004) SDMI-based Rights Management Systems, *Decision Support Systems*, 38(1), 33-46.
- Mulligan, D. K., Han, J., Burstein, A. J. (2003) How DRM-based Content Delivery Systems Disrupt Expectations of "Personal Use". Paper presented at the ACM Workshop On Digital Rights Management, Washington D.C., WA, USA.
- Porter, M. E. Millar, V. E. (1985) How Information Gives You Competitive Advantage, *Harvard Business Review*, 63(4), 149-160.
- Premkumar, G., Ramamurthy, K., Crum, M. (1997) Determinants of EDI Adoption in the Transportation Industry, *European Journal of Information Systems*, 6(2), 107-121.
- Safavi-Naini, R., Nicholas, P. S., Uehara, T. (2004) Import/Export in Digital Rights management. Paper presented at the ACM Workshop On Digital Rights Management.
- Zhu, K., Kenneth, K., Xu, S. (2003) Electronic Business Adoption by European Firms: A Cross-Country Assessment of the Facilitators and Inhibitors, *European Journal of Information System*, 12(4), 251-268.