计算机工程与应用 2007 43 (19): 19-22 ISSN: 1002-8331 CN: 11-2127/TP

博士论坛

OMA DRM标准在嵌入式研发实验中的性能分析

田 捷[1]，张新访[1]，宋翊麟[2]，程 明[3]

1.华中科技大学 信息科学与技术研究所，武汉 430074
2.中国科学院 计算技术研究所，北京 100080
3.清华大学 计算机软件与理论研究所，北京 100084

收稿日期 修回日期 网络版发布日期 2007-6-20 接受日期

摘要 由于数据内容服务在移动业务中起着非常重要的作用，数字版权管理即将成为手持终端一项关键性的部件。对开放移动联盟所定义的数字版权管理开放标准最新版本在手持终端上进行了研发与应用实验，引入了专用硬件模块来处理特定密码学操作，详细分析了其对整体系统性能所起到的重要作用，并对性能指标提升做出了详尽的统计分析。通过对该发布标准的深入分析与探讨，解析了具体实施过程中当受保护数字内容被访问时，相关密码学操作如何被触发及执行过程等细节。通过综合分析分别以软硬件执行特定加解密算法实验后所得到的包括消耗时长在内的统计数据，就能指导架构师在建立系统模型时引入专用硬件处理，从而大大提升系统处理性能及其电池巡航能力。

关键词 专用硬件模块 权利对象 终端代理 密码学操作

分类号

Capability analysis of embedded actualization of OMA DRM II

TIAN Jie[1]，ZHANG Xin-fang[1]，SONG Yi-lin[2]，CHENG Ming[3]

1.Institute of Information Sciences and Technology，Huazhong University of Science and Technology，Wuhan 430074，China
2.Institute of Computing Technology，Chinese Academy of Sciences，Beijing 100080，China
3.Institute of Computer Software and Computing Theory，Tsinghua University，Beijing 100084，China

Abstract

As digital content services gain importance in the mobile world，Digital Rights Management（DRM） applications will become a key component of mobile terminals.This paper examines the effect dedicated hardware macros for specific cryptographic functions have on the performance of a mobile terminal that supports version 2 of the open standard for Digital Rights Management defined by the Open Mobile Alliance（OMA）.Following a general description of the standard，the paper contains a detailed analysis of the cryptographic operations that have to be carried out before protected content can be accessed.The combination of this analysis with data on execution times for specific algorithms realized in hardware and software has made it possible to build a model which has allowed us to assert that hardware acceleration for specific cryptographic algorithms can significantly reduce the impact DRM has on a mobile terminal’s processing performance and battery life.

Key words dedicated hardware rights object terminal agent cryptographic algorithm

DOI:

通讯作者 田 捷 E-mail：tianjie@mail.hust.edu.cn