供方 P 加密内容 $\{M\}_{CEK}$，许可证 $\{CEK,R\}_{PK_D}$，以及许可证签名 σ_{PK_P} 传回设备 D 的 DM。

通过证明挑战，服务提供方 P 相信设备 D 上的 DM 会执行服务提供方 P 送过来的策略，其中指明了数字内容可以被设备 D 访问的条件。为保护策略和秘密信息的私密性，设备 D 使用自己的完整性度量值对其进行封装。加密内容和策略等秘密信息被隔离在 DM 的应用程序域，和其它应用程序的通信都是受到保护的。

4.3.2.2 策略执行

在加密内容和策略等秘密信息分发后，设备 D 上的应用程序或过程即可发起访问请求。设备 D 的 DM 在按照策略信息检查应用程序的完整性状态后产生一个授权决策。对 REL 进行解析后，由应用程序 APP 播放内容。图 5 给出了当设备 D 上的应用程序 APP 访问内容 $\{M\}_{CEK}$ 时的策略执行过程。下面给出该过程描述。

1. APP 向 DM 发送“播放 $\{M\}_{CEK}$”请求。

2. DM 向 APP 发送证明挑战信息。

3. APP 调用 $Attest(H(APP),PK_{APP})$ 响应挑战。

4. DM 将完整性度量值和按照策略期望的值进行比较。如果 APP 是可信的，DM 生成一个会话密钥 k_s，并使用 APP 的公钥加密后，发送给 APP。同时在 DM 内解封 CEK，使用 CEK 解密 $\{M\}_{CEK}$；再使用 k_s 加密 M 后发送给 APP。

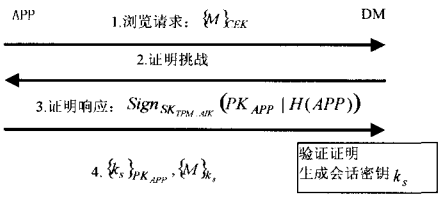

图 5 设备内部的策略执行

4.3.3 安全性分析

通常针对 DRM 系统的攻击有以下 3 种：针对 DRM 协议的攻击；针对客户端设备安全存储的攻击；针对播放应用程序的攻击。其目的都是获取未保护形式的内容产品[9]。针对 DRM 协议的攻击主要攻击的是协议中的客户端和内容提供方之间缺乏相互认证漏洞。针对客户端设备安全存储的攻击通常从安全存储中转储内容密钥或未加保护的内容。针对播放程序的攻击则在使用不安全的程序播放时捕获解密的内容并存储下来。

针对以上问题，基于可信计算的互操作模型提供了以下安全保证：客户端和内容提供方采用远程证明，客户端只有在其度量值得到内容提供方认可的情况下，如：系统已升级并检查没有恶意软件存在等，才可以获取内容产品；客户端得到 cek 和加密内容后存储在受 TPM 保护的 DRM 模块中，杜绝被窃取的危险；内容的解密等操作是在 DRM 模块中完成的，由于 DRM 模块是由 TPM 度量并受 TPM 信任的，因此在此安全环境下的转换同样是可信的。在应用程序度量通过后，通过安全通道传给应用程序播放，而且应用程序之间是相互内存屏蔽隔离的，因而避免其它程序的恶意访问。

结束语 本文针对现有 DRM 系统间实现互操作性的可能性、实施互操作时的技术标准及互操作所使用的协议进行分析，给出了一套在可信计算环境下实施 DRM 互操作的方案，该方案不仅可以实现抵抗现有 DRM 系统中遇到的密钥泄露等攻击，而且为互操作实施过程中内容解密环境提供了安全保证。然而，由于 DRM 系统的复杂性，多种因素尚需要考虑，如权利撤销和迁移等问题，期待在今后的研究中解决。

参 考 文 献

[1] iTunes FairPlay. http://www.apple.com/lu/support/itunes/authorization.html

[2] Microsoft Windows Media Rights Manager. http://www.microsoft.com/windows/windowsmedia/howto/articles/drmarchitecture.aspx

[3] Open Mobile Alliance. http://www.openmobilealliance.org/

[4] 俞银燕，汤帆. 数字版权保护技术综述[J]. 计算机学报，2005，28(12)：1957-1968

[5] Koenen R H, Lacy J, Mackey M, et al. The Long March to Interoperable Digital Rights Management // Proceedings of the IEEE. 2004, 92(6): 883- 897

[6] Reid J F, Caelli W J. DRM, Trusted Computing and Operating System Architecture. Australasian Information Security Workshop 2005 (AISW2005). Newcastle, Australia

[7] Trusted Computing Group. TCG Specification Architecture Overview. Specification Revision 1.2. https://www.trustedcomputinggroup.org, April 2004

[8] The Trusted Computing Group. TPM Main Part 1 Design Principles. February 2005

[9] Taban G, Cardenas A A, Gligor V D. Towards a Secure and Interoperable DRM Architecture // Proceedings of the ACM Digital Rights Management workshop DRM'05. Alexandria, Virginia, USA, 2005: 69-78

重视中、英文摘要的编写

国内外公开发行的标准化科技期刊中的文摘已成为科技论文的重要组成部分，读者可根据文摘提供的信息考虑是否阅读、引用原文；如能被利用，才能体现文章的学术价值，提高原文的引用频次。如此看出学术文章中文摘的重要性，它所起的作用不可替代。

1. 中文摘要一般为 200～300 字，英文文摘的长度一般不超过 250words，不少于 150words。

2. 摘要中不涉及图、表、化学结构式以及非公知公用的符号和术语。关键词一般为 3～8 个，每个关键词首字母大写。

3. 文摘是对文献进行主题分析，以此体现主题概念、主题内容等该篇文献最重要的信息，使读者在没有看到全文的情况下，能够很清楚地了解到该篇文献的中心思想。

4. 文摘语言简洁，避免重复的单元与措辞；文摘中的缩写名称在第一次出现时用全称。文字描述中减少对背景信息的介绍；文摘中不涉及该文献谈及的未来计划；首句不得简单重复题名中已有的信息。

5. 文摘包含的信息量要完整，包括目的、过程及方法、结果三方面内容。英文文摘与中文文摘一致，并使用过去时态叙述作者工作，现在时态叙述作者结论。