1.5 高安全性的 KDM 生成器的设计与实现

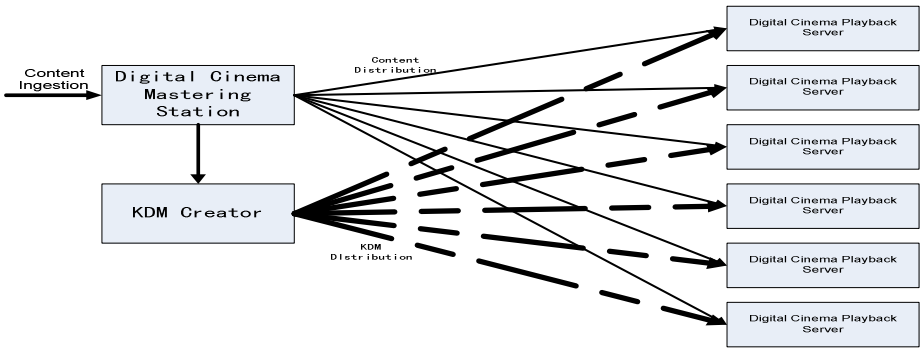
摘要：当前数字电影播放服务器的安全性(内容加密，数字水印，链路加密，物理安全)得到了标准组织以及设备供应商的高度重视与支持。而 KDM 生成器的安全性却没有获得标注组织与设备商的足够重视；但实际上 KDM 生成器的安全性至关重要，因为 KDM 生成器是相关多部影片与多台服务器之间的桥梁，一旦失去安全性损失巨大。本文基于入侵检测机制以及物理安全的设计思路，配合 FIPS140-2 的认证，将 KDM 生成器的安全性提升到同数字电影播放服务器同样的安全高度。

关键字 ：KDM, Digital Certificate, RSA, ECC

一、数字电影工作流程与 KDM 生成器的工作流程

1.1 数字电影工作流程

图 1 给出了数字电影从 DCP 生成，KDM 产生，DCP/KDM 传输到 DCP 放映的全工作流程。



按照当前的实现情况，设备实体分为三个部分：DCP 编码服务器，KDM 生成服务器，以及数字电影播放服务器。DCP 编码器负责完成图像的色彩空间变换，JPEG2000 压缩，图像/音频的 AES 加密，图像/音频的 MXF 打包以及 DCP 生成工作。KDM 生成器通过读取针对它颁发的 KDM 以及各服务器的数字证书完成批量服务器 KDM 生成、管理与维护工作。针对 KDM 生成器而颁发的 KDM 一般由 DCP 编码器完成。数字电影播放服务器通过完成 MXF 解析，数据解密以及 JPEG2000 解压缩并向投影设备与音频设备输出图像与声音而完成播放操作。

对于 DCP 编码服务器尤其是数字电影播放服务器的安全性获得了 DCI/SMPTE 的高度重视，但是对于 KDM 生成器却没有任何安全性的相关要求与实现。究其原因是 DCI/SMPTE 对于播放服务器与 KDM 生成器采用了完全不同的信任模式，对于数字电影播放服务器，他们采取的信任模式是”信任设备不

信任人”；而对于 KDM 生成器他们采取了”信任人”的信任模式。

1.2 KDM 生成器的工作流程

KDM 生成器的主工作流程，见下图：

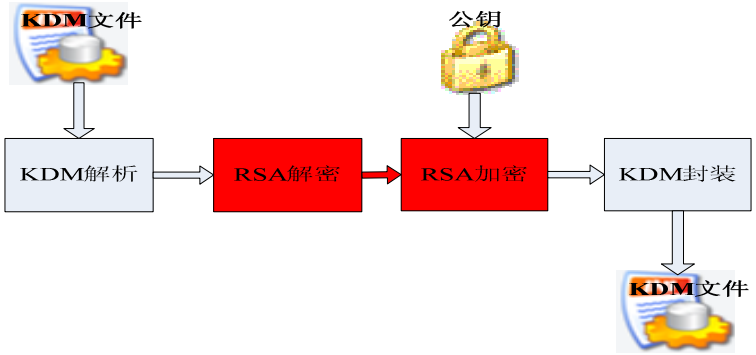


图 2　KDM 生成器的工作流程

1. 把编码器生成的 KDM 输入 KDM 生成器。
2. KDM 生成器对输入的 KDM 进行解析，提取出相关的信息。
3. KDM 生成器把相关的内容用 KDM 生成器的私钥进行 RSA 解密。
4. KDM 生成器批量读入数字电影播放服务器的数字证书，利用数字证书中的公钥对上一步解密出来的信息进行 RSA 加密。
5. 把加密好的信息进行 KDM 封装，输出与各数字电影播放服务器相对应的 KDM 文件。

在上面的处理流程中，KDM 和数字证书是对外公开的，而 KDM 生成器的私钥是需要严格保护的。在好莱坞的安全体系中，私钥的安全级别是最高的，在 DCI 规范中，对板卡上关键信息的保护要求通过 FIPS140-2 认证，并具有入侵检测机制，当发生入侵时，能自动销毁板卡上的关键数据，例如 RSA 私钥。

在 KDM 生成器的整个工作流程中，由于输入的公钥的数量大，并且根据不同的需求，这些所有的公钥有时并不是都需要生成 KDM，怎么才能方便的查询，筛减，选用合适的公钥证书，这就涉及到公钥证书的管理，而管理的最好方式，就是使用数据库对其进行管理。

在生成 KDM 的过程中，也需要全程进行日志记录，以便跟踪回溯，查找以往的操作记录，而生成的 KDM 也需要记录在案，以备查询，同样，这些记录也应使用数据库对其进行管理。

一般 KDM 批量生成的数量都非常大，而 KDM 的生成又涉及 KDM 的解析、RSA 解密、RSA 加密、KDM 生成等工作，所以对生成速度的要求较高。其中比较耗时的运算主要为 RSA 解密、RSA 加密，可以通过硬件加速进行优化。

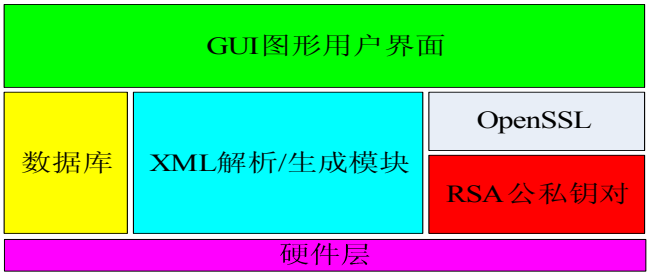
综上所述，一个完善的 KDM 生成软件不但要能读取制作系统提供的 KDM 并分析数据以生成新的 KDM，还要能使用数据库技术对 KDM 以及证书进行存

储与浏览管理。但更重要的仍然是安全性问题。

KDM 生成器可以采用纯软件方案实现，也可以采用 PC 加板卡的硬件方案实现。不管是软件方案和硬件方案，KDM 生成器的工作流程都是一样的，如图 2 ,而唯一不同的是 RSA 解密加密的模块是使用软件实现还是硬件实现以及是否对关键信息使用入侵检测保护机制。

二、KDM 生成器之软件方案

下图是软件方案的系统框图：



在软件方面，KDM 生成器主要由以下几个部分组成：

(1) 顶层 GUI，面向用户的最终界面，用户通过 GUI 来完成 KDM 的生成、存储，浏览管理；服务器证书的浏览管理、存储。

(2)数据库，数据库位于 GUI 的下层，数据库所完成的功能主要就用于实现 KDM 的存储与浏览管理、服务器证书的存储与浏览管理、日志的记录与浏览管理。在软件版中，还有可能用于存储 RSA 的私钥，这也正是该方案的不安全之根源所在之一。

(3)XML 解析生成模块，同样位于 GUI 的下层，主要用于解析/生成 KDM 文件。一般而言，大多数软件使用的都是开源的 xerces 与 xml-security 库。这两个库是 Apache 项目中的组件之一，经过了大规模的应用与长时间的使用。已经被证明是稳定、安全、可靠的。

(4)RSA 模块，位于 GUI 的下层，主要完成 KDM 的加/解密，数字签名以及数字签名的验证。目前绝大多数类似的软件都是使用 OpenSSL 库，OpenSSL 和 Apache 一样属于开源的项目，同样也经过了市场的检验，占领了绝大多数市场份额 ,并且 OpenSSL 还有针对 FIPS140 的版本 ,而在 2K 数字电影服务器和 KDM 生成器中，使用的就是 FIPS140 的版本。重要的一点是，FIPS140 版的 OpenSSL 注重的是算法的安全性，并不涉及算法的保护，也就是说，虽然算法是安全的，但算法的运行平台，存储介质并不在保护范围内。因此黑客可以跟踪调试等手段对它进行拆解。

(5)硬件层，位于最下层，一般来说，是指 X86 通用计算机平台，所有的应用软件及底层库都运行在这个平台上面。

以上是 KDM 生成器的软件方案，我们可以看到，由于其是基于软件实现，并运行在通用平台上，利用现今的技术，很容易就会被破解侵入；同时其私钥存储在未受保护的区域，很容易被窃取，从而使所有的 KDM 安全性失去控制，所以基于软件的方案是毫无安全性可言。

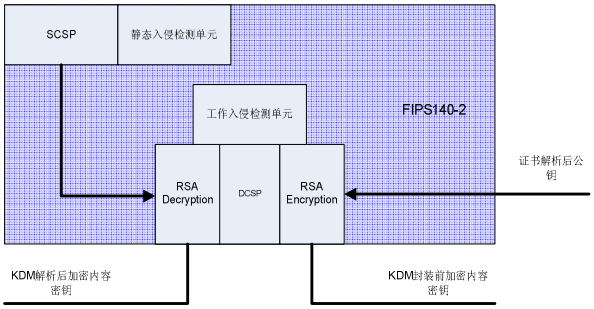
这种不安全的实现方案被大多数 KDM 生成器设备商采用并提供给数字电影制作单位使用，对数字电影的整个产业链构成巨大的安全漏洞。

三、KDM 生成器之硬件方案

硬件实现方案的结构图如图 3 所示，其相对于软件方案突出的区别与优势在于：

(1) RSA 加密、解密操作有板卡上的芯片与电路完成，一方面提高了操作速度，另一方面提高了安全性；(2) 采用将 DCSP(AES 内容密钥)与 SCSP(KDM 生成器私钥)保存在板卡上，并通过入侵检测等机制以保护其安全性。

对于执行 RSA 私钥存储， RSA 加解密操作以及入侵检测的电路我们称之为 KSB(KDM Security Block)，其具体接头如图 4 所示，



所谓的静态入侵检测指的是用来保护本 KDM 生成器自身的私钥等关键信息(SCSP)，而工作入侵检测主要是保护已经被解密的内容密钥(AES 密钥)。

软件层与硬件层之间的通信时通过基于 PCI/PCI-E 协议的 API 进行，概括起来其交互的数据主要包括：

(1) KDM 解析后的加密内容密钥；

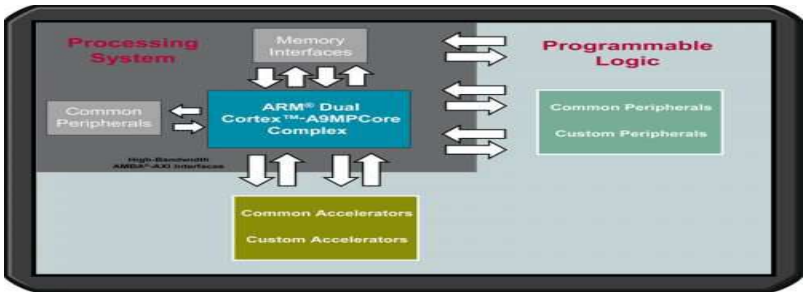
(2) 证书解析后的公钥；

(3) KDM 封装前的加密内容密钥；

一种可选的实现方案是利用 FPGA 中的 Microblaze 或 PowerPC，ARM 等处理器实现 RSA 繁杂的计算工作。下表给出了采用不同架构的对比数据。

处理器		Micral	
Microblaze		xySSL	
ARM		OpenSSL	
PowerPC		OpenSSL	
Logic		Logic	

最优的方案是 ARM 方案，只需要利用 AMBA 总线即可完成 ARM 与 PCI/PCIe 总线的数据交互。



四、RSA 与 ECC

目前主要有三种类型的公开密钥密码系统，分别是基于素数分解的公钥密码系统，例如 RSA，Rabin（Rabin 在 1979 年提出的变型 RSA 算法）等；基于离散对数问题（DLP）的公开密钥密码系统和基于椭圆曲线离散对数问题（ECDLP）的公开密钥密码系统。

离散对数问题（DLP）是找到一个整数 m 以满足

$$Q = P + P + \cdots + P = mP .$$

基于在各种有限群上解决 DLP 问题的困难性，有大量的密码学构造。第一用来构造公钥密码算法的群是（Diffie-Hellman,1976）是一个有限域的乘法群 F_p^*。Koblitz 和 Miller（1985）分别独立建议使用椭圆曲线上点模 p 的群 $E(F_p)$。他们没有发明新的加密算法，但他们是第一个通过椭圆曲线实现了现有的公开密钥密码系统。

一个基于素域主域的 ECC 例子为素域 Z31 上的 E: $y^2 = x^3 + x + 13$，而我们选择基点 P = (9, 10)。 事实证明，#E (Z31) = 34 并且 P 的阶为 34。

K	KP	K	KP	K	KP	K	KP	K	KP	K	KP
1	(9,10)	7	(6,24)	13	(27,10)	19	(5,22)	25	(16,23)	31	(23,12)
2	(18,29)	8	(24,29)	14	(26,21)	20	(26,10)	26	(24,2)	32	(18,2)
3	(23,19)	9	(16,8)	15	(5,9)	21	(27,21)	27	(6,7)	33	(9,21)
4	(4,22)	10	(20,2)	16	(19,3)	22	(28,18)	28	(17,13)	34	*o*
5	(25,16)	11	(22,22)	17	(10,0)	23	(22,9)	29	(25,15)		
6	(17,18)	12	(28,13)	18	(19,28)	24	(20,29)	30	(4,9)		

表 1　素域 Z31 上的 ECC 例子

在同等的安全级别下，ECC 密钥的长度要短于 RSA 密钥的长度，因此 ECC 算法减少了存储空间和降低了计算的复杂性。

Symmetric	56	80	112	128	192	256
RSA n ECC p	512 112	1024 161	2048 224	3072 256	7680 384	15360 512
Key Size Ratio	5:1	6:1	9:1	12:1	20:1	30:1

表 2　ECC 与 RSA 的比较

使用同样长度密钥（或在同等安全级别下运算更快）ECC 算法更安全的原因是没有亚指数算法来解决 ECDLP 的问题，但却有亚指数算法来解决整数分解的问题。

对于数字电影的应用 ,它要求在严格限制存储资源和计算资源的媒体块的安全模块（SM）中实现公开密钥密码。因此 ECC 密钥密码系统比 RSA 密钥密码系统更有优势。

由于公开密钥密码系统是基于数字证书之上的 PKI (公共密钥基础) ，所以需要采用基于 ECC 的数字证书。

数字证书由三部份组成。首先是用户或设备的身份识别信息。其次是公开密钥，私钥由用户自己掌握。最后是数字证书的数字签名。

对于基于 ECC 的数字证书，你只需要改变三个地方。首先要把身份签名算法的类型从 RSA 改为 ECC ,例如 ECDSA 。其次要把公钥信息从 RSA 改为 ECC。最后，用 ECC 签名替代 RSA 签名。

我们力主在数字电影领域使用 ECC 算法取代 RSA 算法。

五、结论

目前大部分 KDM 生成器均不满足安全性的需求，因此以硬件板卡方案为主

的设计方案，结合入侵检测以及 FIPS140-2 认证将成为满足安全性需求的方案。其核心在于入侵检测机制(物理安全)以及公钥密码算法的实现。

为了增强其安全性，我们的设计同时实现了 RSA 算法与 ECC 算法。

六、参考文献

[1] SMPTE 430-1

[2] SMPTE 430-2

[3] SMPTE 430-3

[4] Cinecert

[5] GDC

[6] Qube

[7] Leonis

[8] FIPS140-2

[9] OpenSSL

[10] xySSL

[1] Neal koblitz, A Course in Number Theory and Cryptography, 2nd edition, Springer-Verlag (1994).

[2] Shichao Ma, Research and Design on Real-Time Digital Security Chip, Institute of Computing Technology Chinese Academy Of Sciences, thesis.

[3] PKCS#13, Elliptic Curve Cryptography Standard, http://www.rsa.com/rsalabs.

[4] PKCS #1 v2.1: RSA Cryptography Standard, http://www.rsa.com/rsalabs.

[5] Digital Cinema Initiatives, LLC, Digital Cinema System Specification version 1.2, http://www.dcimovies.com

[6] SMPTE 430-1M, Key Delivery Message, http://www.smpte.org/standards

[7] EDCINE, European Digital Cinema Security White Book, https://www.edcine.org

[8] Gonzalez, I.; Gomez-Arribas, F.J. Ciphering algorithms in MicroBlaze-based embedded systems, Computers and Digital Techniques, IEE Proceedings -Volume 153, Issue 2, 6 March 2006 Page(s): 87 – 92.

[9] Jeffey Bloom, Digital Cinema Content Security and the DCI, Information Sciences and Systems, 40th Annual Conference on Volume, Issue, 22-24 March 2006 Page(s):1176-1181.

[10] D.Hankerson, A.Menezes, S.Vanstone, Guide to Elliptic Curve Cryptography, Springer-Verlag (2007).