



# 数字媒体装置的下一代安全技术

## 一个并不轻松的话题

人们对于应该在何种程度上对音乐、电影和其他数字媒体运用数字版权管理（digital rights management, DRM）的问题的争论达到了白热化的程度。从消费类电子 OEM 的角度来看，几个基本问题是毋庸置疑的。首先，大多数内容的拥有者继续坚持将 DRM 的安全性作为向便携式电子产品 [如媒体播放器（PMP）] 提供优质内容（premium content）的前提条件。OEM 们也有必要在人们使用自己的产品来解锁受保护的数字媒体内容时防备自己不至于成为司法诉讼的对象。

鉴于当前的防复制机制已经被破解，而且破解方法被黑客们贴到了 Web 上，OEM 们所剩下的招数就是力争在他们的装置上实现防篡改能力更强的安全防护功能。当电子商务和社交网络应用也掺和进来时，难度就相应上升。

上述的局面就从两个方面对 OEM 们提出了挑战：如何为其装置吸引到更多的优质内容以扩展生意；同时，如何减少连带责任（liability exposure）以避免财务上的损失。制造商们坚持寻求提高 PMP 和其他装置的安全防护等级的方法，这带来的好处将远远超出 DRM 的应用。

## DRM 方案虽多，却需面对同样问题。

消费类电子 OEM 所面对的一个实际情况是，没有一种 DRM 方案能在任何地方都占尽优势，而且这些方案目前也没有实现兼容性。当前领先的方案包括：FairPlay®（Apple）、Windows Media® DRM 10（Microsoft）和 OMA（Open Mobile Alliance，开放移动联盟）技术。

随着内容的拥有者努力推动更为严格的保护措施采用，在整个业界范围内对于制造符合 DRM 要求的 PMP 和类似装置的要求正变得越来越严格。于是，开发者将不得不在防范性鉴定方面采取更强有力的措施，这将确保只有经过授权的装置才能获取受到保护的媒体或者个人数据。集成的、基于硬件的安全性 - 当前尚未普及 - 在保护私人密钥和密钥的安全交换方面变得必不可少，其目的是保护在下载和上载过程中的数据传送。

要看到另一个趋势：越来越多的消费者被 DRM 弄得十分沮丧。这样的情形正在推动某些内容分发服务商尝试提供无 DRM 管理的内容，特别是在录音行业。消费者和某些技术行业的领先者也在推动新的使用模式的采用，如能够在其所拥有的全部装置上合法地拷贝下载内容。

## 吃上官司的风险

美国数字千年版权法案（Digital Millennium Copyright

Act, DMCA）中的条文在很多方面都牵涉到那些提供可获取媒体内容的装置的制造商们。美国境内出售的产品以及在全世界出售的消费类电子产品，都有可能受到某种法案的约束。DMCA 在 1998 年通过后，许多国家也颁行了类似的法案。

OEM 被夹在两个群体的中间：一边是受到 DMCA 保护的内容所有者，而另一边则是不愿意购买那些无法按自己的方式来使用的产品的消费者。在设计消费类电子时，OEM 事实上必须决定什么才是公平、恰当的使用那些受到保护的内容的方式。限制过严的产品一定卖得不好；而一种招致数字媒体提供商的攻讦的产品，必然使自己的制造商陷入诉讼之中。SonicBlue 就是一个例子：它推出的 ReplayTV 个人视频录像机上的可跳过商业广告和文件共享的功能，遭到了数家广播公司的起诉，吃了这场官司之后，SonicBlue 只好宣布破产

出于让生意蒸蒸日上以及减少风险的考虑，OEM 希望找到能实现装置级的安全保护能力的方法。内容的保护是一个很好的起点，因为它是许多当前所关心的问题的核心。

## 当前 DRM 的实施方式

当前的安全方案一般是基于对数字签名的鉴别这一基本理念，数字签名则使用公共密钥密码的方法来对装置进行鉴别，并对数字内容进行加密以保护数据。这种方法对一个安全的装置来说，意味着相应的设计可以为代码执行和密码资产（如密钥）的保护提供安全可靠的处理环境。

许多 DRM 的实施目前是通过软件或者封装（encapsulation）技术来保护版权管理对象（数字媒体内容）和秘密资产。

纯软件的实现方法可以基于操作系统的安全和非安全环境的隔离来实现。不过，这些实现方法并不安全，因为它们易受到简单的软件攻击和硬件攻击（如使用仿真硬件或者代码注入方法）的破坏。

使用软件来打乱秘密资产是现有的 DRM 具体实施用来隐藏 DRM 密钥的另一种方法。但是内存分析却使得这一技术不再有效。

将秘密资产封装到可信模块（trusted module）中是另外一种常用的办法。虽然可信模块本身可能是安全的，但整个平台却并非安全。黑客们可以在数据出入可信模块的过程中或者当数据还在可信模块之外时通过总线监测和软件攻击的方法来窃取秘密资产。

底线是，无论他们采用软件模糊法还是集成到可信模块内



的方法，现有的DRM的实现无法提供足够保护力，因为它们并不是全面的、整体性的方法。对整个系统进行保护很有必要，Analog Devices的 Blackfin®处理器提供了 Lockbox Secure Technology™，其相应的灵活的功能组合可以被开发者用来在PMP和类似产品上实现安全的DRM和其他保护性措施。

## Blackfin Lockbox 安全防护技术

无论是DRM还是其他方面的需求，考虑在PMP和类似产品上配备装置级安全措施都是很有意义的，这样做有3个目的：内容保护，即确保只有在得到许可的情况下才能使用优质内容；保护秘密，如个人数据和知识产权；装置和用户的身份识别。

Blackfin Lockbox Secure Technology 的设计目标是让 OEM 们能实现上述这些目标。它利用硬件和软件元件保护安全内存空间并只容许经过鉴别的代码来控制各种安全保护功能。

总的来看，Blackfin Lockbox Secure Technology 各组成部分可以提供开发者在满足数字媒体装置安全需求时所需采用的各种重要的功能。

- **来源的验证** - Blackfin Lockbox Secure Technology 可以通过对嵌入一段代码映像的数字签名来对其进行验证，并准备了一个用于识别实体和数据来源的流程。
- **完整性** - 用户可以使用Blackfin Lockbox Secure Technology的数字签名认证流程来确保存储介质的消息或者内容不会以任何方式被改变。完整性可以利用数字签名的鉴定进行检验。
- **机密性** - 密码加密/解密可以服务于必须有防止未经批准的用户看到并使用特定文件和流的情形。Blackfin Lockbox Secure Technology的安全处理环境（安全模式）和安全内存则支持机密保护。

- **可更新性** - Blackfin Lockbox Secure Technology 的芯片专有ID（Unique Chip ID）与一个可信的DRM agent（由OEM采购）结合起来，可以让开发者实现DRM系统的可更新性。

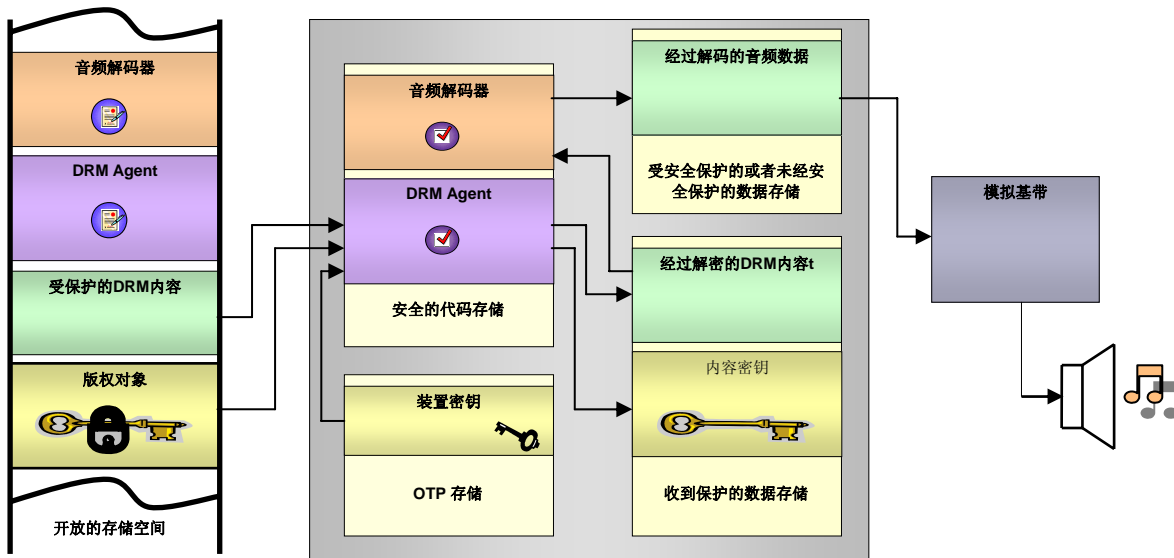
单次可编程（One-time programmable, OTP）的存储器是 Blackfin Lockbox Secure Technology 用来实现这些功能的部件之一。它的位于 OTP 内存中的公开化、非受保护的、用户可编程的区域，适合于存储用于对系统进行鉴定的公共密钥，这种存储方式应该可以由 OEM 来控制 and 定义。OTP 存储器的一个私人性的、受到安全保护的、可由用户编程的区域则让开发者对它们自己私有装置的资产（如私有密钥）进行编程并维持这些资产的机密性和完整性。私有的、安全的 OTP 存储只有通过 Blackfin 的安全模式才能访问，这种模式只有在数字签名鉴定流程完成后才能进入。

安全模式使得系统的具体实施中只有经过鉴定的、受到信任的代码能执行 DRM 操作或者关键性的子集，如证书的处理或者版权对象的处理。存储保护为解密后的 DRM 内容和内容的解读密钥提供了安全的存储。

与 DRM 相关的一些特有的优点是什么？全面运用 Blackfin Lockbox Secure Technology 的所有功能的话，开发者就可以通过安全的鉴定过程以及对器件 ID 和控制对数字媒体文件的访问性的 DRM 密钥的不断更新，来提高对优质内容的非经认证的使用的防护水平。使用私有的、安全的 OTP 存储区域和安全模式可以大大增加将 DRM 从数字媒体中除去的难度，从而把一个普通的装置变换成一个先进的、带安全防护的装置。

## DRM 实施方法示例

下面举例予以说明。下图示出如何利用 Lockbox Secure Technology 在便携式音频播放器中实现 DRM 的可能方法。在这一虚构的实现方案中，DRM agent 和音频解码器





已经得到了厂商的数字签名，因此可获得人们信任，从而能在受到安全保护的平台上运行。

在经历了数字签名鉴定过程后（来源验证和完整性），DRM agent 赢得了“受信任的代码”的地位，从而有权访问受保护的环境（包括受保护的 OTP 存储）。在典型的 DRM 架构中，DRM 利用用该装置存储在受保护的 OTP 存储中的私有密钥来从版权对象中提取用于对音频内容进行解密所需的内容密钥。内容密钥可以安全地存储在受保护的数据存储区中，在这里它仍然不会被那些未得到信任的代码访问。DRM agent 使用内容密钥来对受到保护的 DRM 内容进行解密，并将解密后的内容存入受到安全保护的数据存储中。

音频解码器经过了签名的验证，以赢得“可信代码”的地位。一旦通过验证，音频解码器就被授予访问受保护环境的许可。它可以对加密后的音频内容进行解码，并将所生成的音频样本存储到受到保护的或者不受保护的存储区中，具体到哪个区域，则取决于要求和可获得的存储空间。

## IP、电子商务、社交网络与个人数据保护

在器件级上支持 DRM 的一种更完善的办法与用 Blackfin Lockbox Secure Technology 可以实现的一个目标是相一致的。对于消费类电子的制造商来说，保护自己的知识产权（IP）的防护措施是优先要考虑的问题，Lockbox Secure Technology 的功能为实现这方面的功能提供了一个有效的机制。Lockbox Secure Technology 存储芯片专有 ID（Unique Chip ID）的能力可以让开发者将自己的软件锁在装置中，以防止当装置被人仿冒时这些代码被复制和复用。OEM 还可以利用 Blackfin 的安全模式来维持机密性和防止 IP 盗用。

另外，通过采用 Lockbox Secure Technology 而实现的更优化的器件鉴定能力，可以支持得到充分保护的电子商务和社交网络的端一端文件共享。举例来说，OEM 可以容许消费者合法地截取受到保护的内容的样本并提供给自己的朋友，以此来运用能在装置层次上实现的更高的安全性。

若使用 Lockbox Secure Technology 来实现更安全的密钥处理，则可以建立安全的通信会话，以便在下载和上载过程中保护数据的传输。

OEM 们也有机会利用 Lockbox Secure Technology 来保护个人数据。消费者可以对自己个人数据的安全性有更强的信心，在得到正确授权的装置上购物或者在个人的社交网络上共享信息。例如，安全性可以得到扩展，以包括装置上的数字身份管理。装置的丢失并不一定会危及个人信

息。只要消费者用恰当的口令锁定装置的话，鉴别功能就可以让私人数据免受窥测。

正如对连接到 Internet 的 PC 提供加密保护协议（SSL 和 S-HTTP）使得电子商务在 1990 年代开始兴旺起来，一旦这样的安全鉴别和处理能力能在 PMP 和类似产品上启用的话，就可以搭建一个舞台，让这些装置可以实现的服务和处理的内容得以快速增长。

## 消费者的满意程度

再回到 DRM 的话题。涉及多种产品的 OEM 们可以利用在他们的生态系统中处处运用 Blackfin Lockbox Secure Technology，对所有的经过批准的装置进行检验，维持所需的版权保护，而不必付出分别在每个装置上采用安保 ID 芯片的开销。举例来说，这将支持这样的一种使用模式：拥有恰当授权的产品的消费者可以无缝地将一支防复制的歌曲从他的 PMP 转移到他的 MP3 时钟收音机上。

Blackfin 的可编程性还使得它适用于另一种情形。Blackfin 的指令集能实现多种多样的软件加密算法，这就使得相同的装置能支持多种内容保护格式。当 OEM 能保证授权许可的安全性的情况下，PMP 可以支持由不同的数字音乐和视频零售商所使用的 DRM。数字娱乐的狂热爱好者们将能在他们的消费电子装置之间转移合法下载的音乐和电影。

## 确保商机

OEM 们可以运用 Blackfin Lockbox Secure Technology 的威力来将 PMP 和其他的产品推进到消费类电子的装置的安全保护的最前沿。采用私有密钥和 Blackfin Lockbox Secure Technology 的安全处理模式之后，OEM 可以让他们的系统安全性优于当前的那些仅仅对部分系统进行安全保护的系统。从 DRM 到 IP 保护，再到电子商务、社交网络、个人数据，开发者们都可灵活地应用更有效的安全防护措施，从而减少被起诉的危险，同时支持令消费者高兴的功能特色和不同的商业模式。

同时，Blackfin 可以实现低功耗化，并完成控制与信号处理的融合、外设的集成、鲁棒的开发环境和低廉的物料管理（bill of materials）成本，这些构成了成功的数字媒体装置设计所需的嵌入式的处理套装。