The Next Generation of Secure Technology for Digital Media Devices

An Uneasy Piece

Debate runs hot about the extent to which digital rights management (DRM) ought to be applied to music, movies, and other digital media. From the perspective of the consumer electronics OEM, a few fundamentals are beyond dispute. First, most content holders continue to insist on secure DRM as a condition for making premium content available on portable electronics such as media players (PMPs). And OEMs have the need to protect themselves against legal action when people use their products to unlock protected digital media content.

Being that current copy protection mechanisms have been cracked and the hacks posted on the Web, OEMs are left to grapple with implementing more tamper-resistant security in their devices. The difficulty increases when e-commerce and social networking applications enter the mix.

That leaves OEMs with challenges on two sides: attracting more premium content for their devices to grow the business, and reducing liability exposure to avoid financial loss. Manufacturers stand to benefit by finding a means to upgrade PMPs and other digital media devices to a more secure status, and the advantages go much further than DRM.

Many DRM Schemes, Same Issues

Consumer electronics OEMs face the reality that no single DRM scheme prevails everywhere, nor are these schemes currently compatible with each other. Among the leaders today are FairPlay® (Apple), Windows Media® DRM 10 (Microsoft), and OMA (Open Mobile Alliance) technologies.

Requirements for building DRM-compliant PMPs and similar devices are also becoming more rigorous across the industry as content owners drive for tougher protection. As a result, developers will have to implement stronger measures in areas including secure authentication, which ensures that only authorized devices have access to protected digital media or personal data. Integrated hardware-based security–not common today—will be necessary to protect private keys and process key exchanges securely, in order to protect data transfer during downloads and uploads.

Another trend to watch: growing consumer frustration with DRM. The situation is prompting some content distribution services to experiment with DRM-free content, particularly in the recording industry. Consumers and some technology industry leaders are likewise pushing for new usage models, such as the ability to copy legally downloaded content on all of their devices.

Exposed to Liability

The Digital Millennium Copyright Act (DMCA) has tremendous implications for OEMs that supply devices for accessing digital media content. That's as likely true for products sold in the U.S. as for consumer electronics sold around the world. Many nations put similar legislation in place after the DMCA was passed in 1998.

OEMs stand in the middle between content owners with DMCA on their side, and consumers, who are unwilling to buy products they cannot use in ways they wish. In designing consumer electronics, OEMs in effect must determine what constitutes fair and appropriate use of protected content. A product that is too limited will not sell well; one that meets with objections from digital media providers will land its manufacturer in a lawsuit. SonicBlue, for example, went bankrupt after a suit in which broadcasters cited the commercial skipping and file sharing features of its ReplayTV personal video recorder.

For reasons of business growth as well as risk reduction for the OEM, better approaches to device-level security are desirable. Content protection is a good starting point because it is at the center of many of today's concerns.

DRM Implementations Today

Security schemes today are typically based upon the concept of authentication of digital signatures that use a public-key cipher to authenticate the device, and encrypt digital content to protect the data. This method provides for a secure device to the extent the design provides a secure processing environment in which to execute code and protect secret assets such as keys.

Many DRM implementations currently use software or encapsulation techniques to protect rights-managed objects (digital media content) and secret assets.

Software-only implementations may rely on the operating system's separation of secure and nonsecure environments. However, these implementations are not secure because they are susceptible to simple software attacks as well as hardware attacks, such as the use of emulation hardware or code-injection methods.

Using software to obfuscate secret assets is another method that existing DRM implementations use to hide DRM keys. However, memory analysis renders this technique ineffective.

Encapsulation of secret assets in trusted modules is another approach often employed. While the trusted module itself may be secure, the platform as a whole is not. Hackers may carry out bus monitoring and software attacks to steal the secret assets during transport to and from the trusted module, or while outside the trusted module.

The bottom line is that whether they employ software obfuscation or incorporate trusted modules, existing DRM implementations fail to provide enough protection because they do not take a holistic approach. Protecting the whole system is necessary, and Analog Devices Blackfin® processors offer Lockbox™ Secure Technology to provide a flexible feature set developers can use to implement secure DRM and other protective measures on PMPs and similar products.

Blackfin Lockbox Secure Technology

Whether for DRM or other needs, it's useful to think of the device-level security for PMPs and similar products as having three main purposes: content protection that allows only permitted uses of premium content, safeguarding secrets such as personal data and intellectual property, and verifying the identity of devices and users.

Blackfin Lockbox Secure Technology is designed to enable OEMs to achieve these purposes. It uses hardware and software components to protect secure memory spaces and restrict control of security features to authenticated code.

Together, the Blackfin Lockbox Secure Technology components provide important capabilities that developers need in order to address security requirements in digital media devices:

- Origin Verification—Blackfin Lockbox Secure Technology allows for verification of a code image against its embedded digital signature, and provides for a process to identify entities and data origins.
- Integrity—Developers can use a Blackfin Lockbox Secure Technology digital signature authentication process to ensure that the message or the content of the storage media has not been altered in any way. Integrity can be verified using authentication of digital signatures.
- Confidentiality—Cryptographic encryption/decryption supports situations that require the ability to prevent unauthorized users from seeing and using designated files and streams. Blackfin Lockbox Secure Technology's secure processing environment (secure mode) and secure memory support confidentiality.
- Renewability—The Blackfin Lockbox Secure Technology Unique Chip ID, in combination with a trusted DRM agent (sourced by the OEM), enables developers to implement renewability in DRM systems.

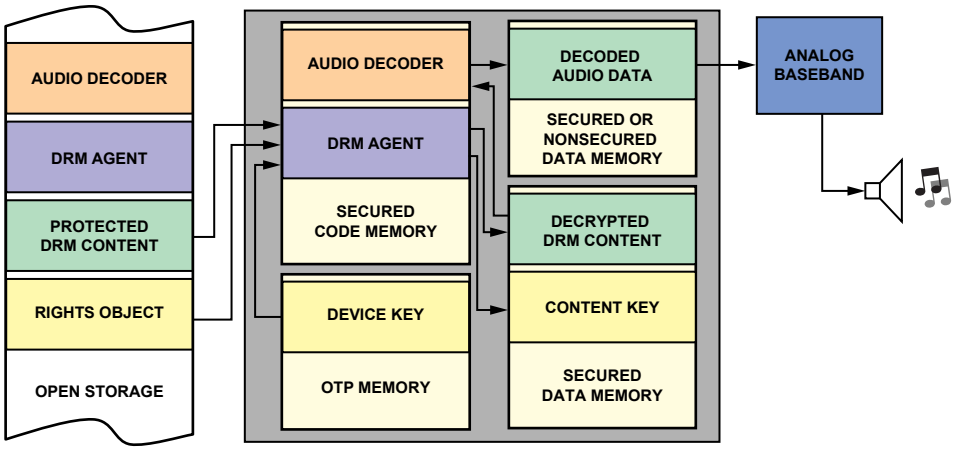
One-time programmable (OTP) memory is one of the components that Blackfin Lockbox Secure Technology uses to enable these capabilities. Its public, nonsecure, user-programmable area of OTP memory is suited for storing public keys to authenticate the system in a manner that is controllable and configurable by the OEM. A private, secure, user-programmable area of OTP memory lets developers program their own private device assets such as private keys, and maintain the confidentiality and integrity of those assets. Private, secure OTP memory is only accessible through the secure mode on Blackfin, which can be entered only by completing a digital signature authentication process.

Secure mode allows systems to be implemented in which only authenticated, trusted code can perform DRM operations or critical subsets such as license handling or rights object handling. Memory protection provides secure storage for decrypted DRM content and content decryption keys.

What are some of the advantages in relation to DRM specifically? With the full set of Blackfin Lockbox Secure Technology capabilities at their service, developers can increase protection against unauthorized use of premium content by securely authenticating and, if necessary, renewing device IDs and the DRM keys that control access to digital media files. Using the private, secure OTP memory area and secure mode substantially increase the difficulty of removing DRM from digital media, turning an ordinary device into a leading-edge secured device.

Sample DRM Implementation

As an example, the following diagram shows how DRM might work using the Lockbox Secure Technology in a portable audio player. In this hypothetical implementation, the DRM agent and the audio decoder have been digitally signed by the vendor and are therefore trusted to run on the secure platform.



After undergoing a digital signature authentication process (origin verification and integrity), the DRM agent earns a trusted code status and is then granted access to the secured environment (including the secure OTP memory). In a typical DRM architecture, the DRM agent uses the device's private key stored in secure OTP memory to extract—from the rights object—the content key necessary for decrypting the audio content. The content key may be safely stored in secured data memory where it remains beyond the reach of nontrusted code. The DRM agent uses the content key to decrypt the protected DRM content and stores the decrypted content into secured data memory.

The audio decoder undergoes a signature verification process to earn a trusted code status. Once verified, the audio decoder is granted access to the secured environment. It decodes the decrypted audio content and stores the generated audio samples either in secured or nonsecure memory, depending on requirements and available storage.

IP, E-Commerce, Social Networking, and Personal Data Protection

An improved way to support DRM at the device level is just one goal that developers can achieve using Blackfin Lockbox Secure Technology. Safeguarding their own intellectual property (IP) protection is a priority for consumer electronics makers, and Lockbox Secure Technology features provide effective mechanisms for doing so. The ability of Lockbox Secure Technology to store a unique chip ID allows developers to lock their software to the device to prevent duplication and reuse of the code in an imitation. OEMs can additionally use Blackfin secure mode to maintain confidentiality and thwart IP theft.

What's more, the improved device authentication possible by employing Lockbox Secure Technology supports fully protected e-commerce and peer-to-peer file sharing for social networking. OEMs can use the greater security possible at the device level by allowing consumers to legally sample protected content to their friends, for example.

And by using Lockbox Secure Technology to implement more secure processing of keys, secure communication sessions can be established to protect data transfer during downloads and uploads.

OEMs also have the opportunity to leverage Lockbox Secure Technology for safeguarding personal data. Consumers could then have increased confidence their personal data would be safe when they make purchases on appropriately enabled devices, or share information in their social networks. For instance, security can be extended to include digital identity management on the device. A lost device also won't necessarily lead to personal information being compromised. Provided the consumer locks the device down with a proper password, authentication can keep private information from prying eyes.

Much as e-commerce blossomed in the 1990s when cryptographically secure protocols (SSL and S-HTTP) became available for PCs connecting to the Internet, once such secure authentication and processing capabilities are enabled in PMPs and similar products, the stage will be set for more services and content to proliferate to these devices.

Consumer Satisfaction

Returning to the topic of DRM, OEMs with multiple products could use Blackfin Lockbox Secure Technology across their ecosystems to verify all authorized devices and maintain the required copy protection without the expense of using separate secure ID chips in each one. This would support a usage model, for example, in which a consumer with suitably enabled products could seamlessly move a copy-protected song from his PMP to his MP3 clock radio.

The programmability of Blackfin lends itself to another scenario as well. Blackfin instruction sets are capable of implementing a variety of cryptographic algorithms in software, which allows the same device to support multiple content protection formats. In cases where the OEM can secure licensing, a PMP might support DRM used by different digital music and video retailers. Digital entertainment aficionados would then be able to move legally downloaded music and movies between their consumer electronics devices.

Securing Business Opportunities

OEMs can apply the strength of Blackfin Lockbox Secure Technology to advance PMPs and other products to the forefront of device security in consumer electronics. With the protection of private keys and secure processing modes in Blackfin with Lockbox Secure Technology, OEMs can make their systems more secure than today's implementations that protect only part of the system. From DRM, to IP protection, to e-commerce, to social networking, to personal data, developers gain the flexibility to put more effective safeguards in place that reduce exposure to liability while supporting consumer-pleasing features and different business models.

At the same time, Blackfin provides the low power performance, converged control and signal processing, peripheral integration, robust development environment, and economical bill of materials (BOM) cost that complete the embedded processing package for successful digital media device designs.

Analog Devices, Inc.
Worldwide Headquarters
Analog Devices, Inc.
One Technology Way
P.O. Box 9106
Norwood, MA 02062-9106
U.S.A.
Tel: 781.329.4700
(800.262.5643,
U.S.A. only)
Fax: 781.461.3113

Analog Devices, Inc.
Europe Headquarters
Analog Devices, Inc.
Wilhelm-Wagenfeld-Str. 6
80807 Munich
Germany
Tel: 49.89.76903.0
Fax: 49.89.76903.157

Analog Devices, Inc.
Japan Headquarters
Analog Devices, KK
New Pier Takeshiba
South Tower Building
1-16-1 Kaigan, Minato-ku,
Tokyo, 105-6891
Japan
Tel: 813.5402.8200
Fax: 813.5402.1064

Analog Devices, Inc.
Southeast Asia
Headquarters
Analog Devices
22/F One Corporate Avenue
222 Hu Bin Road
Shanghai, 200021
China
Tel: 86.21.5150.3000
Fax: 86.21.5150.3222

Printed in the U.S.A. T06666-0-3/07

ANALOG DEVICES