

- Overview
- Background
- Executives
- Investors
- Customers
- News
  - News Releases
  - Media Kit
  - In the News
  - Security News
- Events
- Careers

- EVALUATE PRODUCT
- PRINT PAGE
- EMAIL PAGE
- SALES INQUIRY

## Certicom launches Security Solution for Digital Rights Management (DRM)

Comprehensive Platform Achieves Robust DRM Implementations by Securing Device from Silicon up to the Application

"Certicom understands that the best defense against hackers is to protect the many levels of vulnerabilities throughout an entire system, using hardware wherever possible." -- Al Hawtin, Elliptic Semiconductor

**Find out more**

Fill out our **Online Request Form** to get more information, or call us today.

Fill out our **Online Evaluation Request Form** to get access to a 30-day trial.

Wendy Bissonnette  
Tel.: +1-613-254-9258  
[sales@certicom.com](mailto:sales@certicom.com)

MISSISSAUGA, Ontario – (December 6, 2005)– Certicom today announced Certicom Security for DRM, a comprehensive solution that implements digital rights management (DRM) agents as part of a trusted platform. To achieve DRM robustness, device manufacturers must ensure that only trusted applications have access to DRM resources, and that sensitive keying material is protected and inaccessible. Without this level of security, a DRM scheme could be thwarted by attacks on system resources from downloads of malicious code.

Certicom delivers DRM robustness for multimedia capable mobile phones, handheld devices, consumer electronic devices, and set-top boxes with a platform that includes the Certicom Security Architecture and Certicom KeyInject. Certicom Security Architecture secures device software and leverages hardware-based security in silicon. It includes a pre-integrated Open Mobile Alliance (OMA) DRM Agent from Beep Science and is extensible to other DRM schemes. Certicom KeyInject monitors and controls keying material during device manufacture.



Through a new partnership with Elliptic Semiconductor, Certicom also offers pre-integrated hardware intellectual property (IP) cores that enable chip designers to include hardware-based security for DRM in their own media co-processor designs. With these IP cores, processor designers can exploit the performance and security benefits derived from implementing cryptography and key management functions in hardware. For device manufacturers using off the shelf silicon, Certicom offers board support packages that leverage hardware security available in leading chipsets from Intel and Freescale Semiconductor.

"Certicom understands that the best defense against hackers is to protect the many levels of vulnerabilities throughout an entire system, using hardware wherever possible," said Al Hawtin, vice president of sales and marketing at Elliptic Semiconductor. "When you approach security from a system perspective, our partnership with Certicom is a natural one that offers many security and performance benefits to device manufacturers and multimedia chip developers."

"Certicom's approach to DRM eliminates vulnerabilities that aren't typically addressed by other DRM solutions," said Jim Alfred, director of product management at Certicom. "By protecting the silicon, software components and even the manufacturing environment, we enable vendors to meet DRM robustness rules and protect their investment and revenue."

Certicom Security for DRM includes the following modules:

### Certicom Security Architecture

- Beep Science OMA DRM Agent and Server: fully compliant with the DRM standard from the Open Mobile Alliance (OMA)
- Security Builder ETS: leverages hardware-based key storage, management and cryptographic operations which contribute to robust DRM solutions
- Security Builder Crypto: optimized software crypto provider for cases where a hardware crypto provider is not available, or to complement a hardware crypto provider when all required functions are not available
- Security Builder BSP: interface to specific hardware components including Elliptic Semiconductor IP cores and industry leading chips, including those from Freescale and Intel
- Security Builder API: a common application programming interface that maximizes portability and code re-use from one chip to another
- Elliptic Semiconductor IP Cores: series of hardware cores that allow designers to achieve performance and security benefits by implementing the crypto required by DRM in hardware

### Certicom Key Inject

- provides a mechanism to secure the keys and certificates during the manufacturing process by controlling access to, and reporting usage of, keying information

Certicom Security for DRM with the Elliptic Semiconductor IP Cores is available this quarter. For more information, visit [www.certicom.com/drm](http://www.certicom.com/drm).

#### **About Certicom**

Certicom protects the value of your content, software and devices with government-approved security. Adopted by the National Security Agency (NSA) for classified and sensitive but unclassified government communications, Elliptic Curve Cryptography (ECC) provides the most security per bit of any known public-key scheme. As the undisputed leader in ECC, Certicom security offerings are currently licensed to more than 300 customers including General Dynamics, Motorola, Oracle, Research In Motion and Unisys. Founded in 1985, Certicom's corporate offices are in Mississauga, ON, Canada with worldwide sales headquarters in Reston, VA and offices in the US, Canada and Europe. Visit [www.certicom.com](http://www.certicom.com)

Certicom, Certicom Security Architecture, Certicom Trust Infrastructure, Certicom CodeSign, Certicom KeyInject, Security Builder, Security Builder API, Security Builder BSP, Security Builder Crypto, Security Builder ETS, Security Builder GSE, Security Builder IPsec, Security Builder NSE, Security Builder PKI and Security Builder SSL are trademarks or registered trademarks of Certicom Corp. All other companies and products listed herein are trademarks or registered trademarks of their respective holders. .

#### **Forward-Looking Statements**

Except for historical information contained herein, this news release contains forward-looking statements that involve risks and uncertainties. Actual results may differ materially. Factors that might cause a difference include, but are not limited to, those relating to the acceptance of mobile and wireless devices and the continued growth of e-commerce and m-commerce, the increase of the demand for mutual authentication in m-commerce transactions, the acceptance of Elliptic Curve Cryptography (ECC) technology as an industry standard, the market acceptance of our principal products and sales of our customer's products, the impact of competitive products and technologies, the possibility of our products infringing patents and other intellectual property of fourth parties, and costs of product development. Certicom will not update these forward-looking statements to reflect events or circumstances after the date hereof. More detailed information about potential factors that could affect Certicom's financial results is included in the documents Certicom files from time to time with the Canadian securities regulatory authorities.

The shares of the company described above have been offered only to qualified institutional buyers in reliance on Rule 144A under the Securities Act of 1933, as amended (the "Securities Act"), and outside the United States pursuant to Regulation S of the Securities Act. The shares have not been registered under the Securities Act and may not be offered or sold in the United States or to a U.S. Person absent registration or an applicable exemption from registration requirements.

This press release does not constitute an offer to sell or the solicitation of an offer to buy any security and shall not constitute an offer, solicitation or sale in any jurisdiction in which such offering would be unlawful.

---

For further information, please contact:

**For Certicom**  
Tim Cox  
ZingPR  
(650) 369-7784  
[tim@zingpr.com](mailto:tim@zingpr.com)

Brendan Ziolo  
Certicom Corp.  
(613) 254-9267  
[bziolo@certicom.com](mailto:bziolo@certicom.com)

---