

FOR IMMEDIATE RELEASE

No. 2365

Product Inquiries:

Takeshi Chikazawa
Information Technology R&D Center
Mitsubishi Electric Corporation
Tel: +81-467-41-2181
chika@iss.isl.melco.co.jp

Media Contact:

Travis Woodward
Public Relations Department
Mitsubishi Electric Corporation
Tel: +81-3-3218-2346
Travis.Woodward@hq.melco.co.jp
<http://global.mitsubishielectric.com/news/>

MITSUBISHI ELECTRIC ANNOUNCES ITS 64-BIT BLOCK CIPHER ALGORITHM, 'MISTY', TO BE ADOPTED IN ISO/IEC STANDARD

Tokyo, May 26, 2005 – Mitsubishi Electric Corporation (President and CEO: Tamotsu Nomakuchi) announced today that the 64-bit block cipher algorithm it has developed, MISTY¹, will be used as an international standard in ISO/IEC². It was chosen because of its recognition as a particularly safe and practical method of encryption.

¹A 64-bit block cipher algorithm with a 128-bit encryption key developed by Mitsubishi Electric

²International Organization for Standardization / International Electrotechnical Commission

ISO has been standardizing its information security signature algorithm and authentication mechanism, but not cipher algorithms. There has been a world wide interest in creating such a standard, and in 2000 began development of an international standard for cipher algorithms. Fifteen cipher algorithms from 7 different countries (Canada, Belgium, Japan, Korea, Sweden, Switzerland, and USA) were reviewed by third parties (NESSIE, CRYPTREC, etc) etc. for their safety and applicability (in processing performance and hardware/software areas). MISTY was among 6 other types from 4 different countries to be adopted as a cipher algorithm standard.

Mitsubishi Electric has been strongly promoting the information security business since MISTY1 was publicized in 1996. In 2000, KASUMI, a variant of MISTY, was adopted as the mandatory standard for the

3G mobile systems W-CDMA. MISTY is now internationally acknowledged as a safe and practical cipher. Also in 2000, Mitsubishi Electric and NTT jointly designed Camellia. Mitsubishi Electric is currently offering these algorithms to various standardization bodies such as the ISO, NESSIE and CRYPTREC for proposal. The Japan Ministry of Public Management, Home Affairs, Posts and Telecommunications and the Ministry of Economy, Trade and Industry have officially approved MISTY1 and Camellia for Japanese governmental use. NESSIE (New European Schemes for Signatures, Integrity and Encryption: a three-year project funded by the European Commission and organized by European researchers of cryptography) has also approved these two algorithms. Mitsubishi Electric's encryption technology will become widely used on a global scale. Camellia will also be used in the international standard at the same time.

Mitsubishi Electric's encryption technology development timeline:

1994 January	Linear cryptanalysis is invented
1994 August	World's first experimental DES cryptanalysis
1995 September	MISTY published
1995 November	MISTY registered to ISO9979
1998 August	Royalty free licensing of the MISTY patent
2000 January	KASUMI adopted as W-CDMA standard cipher
2000 March	Camellia (NTT and Mitsubishi Electric) published
2001 May	MISTY and KASUMI IP License
2002 July	KASUMI adopted in the GSM system
2003 February	MISTY1 and Camellia approved for use in Japanese "e-government"
2003 February	MISTY1 and Camellia approved in the NESSIE project
2003 July	CRESERC (implementation scheme for Elliptic Curve signature ECDSA) developed (NTT, Hitachi Ltd., and Mitsubishi Electric)
2005 May	MISTY1 adopted in ISO/IEC standard

MISTY

MISTY was developed by Mitsubishi Electric in 1995 and is a family name of two encryption algorithms MISTY1 and MISTY2, which has the world's highest-level of security and practicability. MISTY1 and MISTY2 are both a 64-bit block cipher with a 128-bit key, which can be used for data communication and

electronic commerce in open networks. The MISTY specifications have been published in full.

Kasumi

A customized version of the MISTY1 cipher algorithm for cellular phones. In 2000, it was used in third generation cellular phones (W-CDMA) as a global standard.

Camellia

Camellia is a next-generation 128-bit block encryption algorithm jointly developed by Mitsubishi Electric and NTT, and supports three key sizes: 128, 192 and 256 bits. The Camellia specifications have been published in full. Camellia was designed not only for high security levels suitable for the next generation but also for high performance in any target platform such as embedded systems, where low power consumption is mandatory and server computers, where utmost speed is a top priority.

NESSIE (New European Schemes for Signatures, Integrity, and Encryption)

A project financed by the European Commission to form a consensus between business and academia. MISTY1 is the only cipher in the 64 bit block, and along with Camellia in the 128-bit block category, are officially approved by both NESSIE and the US government's Advanced Encryption Standard (AES)

About Mitsubishi Electric

With over 80 years of experience in providing reliable, high-quality products to both corporate clients and general consumers all over the world, Mitsubishi Electric Corporation (TSE:6503) is a recognized world leader in the manufacture, marketing and sales of electrical and electronic equipment used in information processing and communications, space development and satellite communications, consumer electronics, industrial technology, energy, transportation and building equipment. The company recorded consolidated group sales of 3,410 billion yen (US\$ 31.9billion*) in the fiscal year ended March 31, 2005. For more information visit <http://global.mitsubishielectric.com>

*At an exchange rate of 107 yen to the US dollar, the rate given by the Tokyo Foreign Exchange Market on March 31, 2005.