FOR IMMEDIATE RELEASE

Hitachi's light-weight "*Enocoro*" stream cipher adopted as an ISO/IEC standard

Tokyo, October 1, 2012 - Hitachi, Ltd. (TSE:6501, "Hitachi") today announced that "*Enocoro*" a light weight stream cipher(1) developed by Hitachi in 2007, has received final approval by ISO/IEC and has been adopted as an ISO/IEC29192(2) standard. Compared to AES(3) the current *de facto* standard for data encryption, *Enocoro* achieves the encryption process with about one-tenth the amount of power consumption. Due to this feature, it is able to provide the basic security functions for compact control equipment and sensors used in important infrastructure(4), at a low cost. This cipher is an extended development of research results from work commissioned by the National Institute of Information and Communications Technology (NICT, Japan) under their FY 2005-2007 project entitled "R&D for the safe circulation and storage of mass data."

In recent years, not only PCs and mobile phones but a wide range of equipment such as consumer electronics and motor vehicles, are being connected to the Internet via compact devices such as RFID(5) and sensors with wireless communication functions to exchange various information. At the same time, the risk of information leakage on the Internet, as seen with computer viruses, is increasingly on the rise. Thus, increased security will be necessary even for compact devices with limited information processing resources in their CPU or memory, and low power consuming technology enabling encryption of data and authentication of devices as well as low-cost implementation of these functions is vitally needed. The International Organization for Standardization (ISO) and the International Electro technical Commission (IEC) have been working on ISO/IEC 29192 as an international standard for light-weight cryptography for implementation in constrained environments and have now issued ISO/IEC 29192-3, the section on stream ciphers, adopting *Enocoro* as an international standard.

Since developing *MULTI-2* in 1989, Hitachi has continued research in cryptography and standardization of the technology. In recent years, the stream ciphers *MULTI-S01*(6) and *MUGI*(7) in 2005, and the public key cipher *HIME(R)*(8) in 2006, have been adopted as international standards. With the adoption of *Enocoro* this time, four cryptographic algorithms developed by Hitachi have become standards. Through its cipher technology including *Enocoro*, Hitachi will continue research on technologies for a reliable networked society to improve security as important infrastructure and industrial systems become increasingly connected.

Notes

(1) Stream cipher: A cryptographic method which encrypts data bit by bit using a random bit stream (key stream) generated by means of a private key.
(2) ISO/IEC 29192 (Light-weight cryptography): An encryption standard for implementation in constrained environments. The standard consists of 4 parts: 1) General, 2) Block ciphers, 3) Stream ciphers, and 4) Mechanism for using public key cryptography. Part 1 and Part 2 were

issued on 29th May 2012 and 10th January 2012, respectively.

(3) AES (Advanced Encryption Standard): An encryption standard adopted by the US government in 2001, and the de facto world standard for data encryption. AES was ratified after 3 years of open public assessment sponsored by the National Institute of Standards and Technology (NIST).

(4) In the "Phase 2 action plan for information security measures concerning critical infrastructure" (3rd February 2009, Information Security Policy Council of the Information Security Center, Cabinet Office of Japan), "critical infrastructure" is defined as platforms formed by business entities providing highly irreplaceable services essential in the daily lives of citizens and for socio-economic activity; which if suspended, reduced or become unavailable, has the potential to greatly disrupt the lives of citizens and the socio-economic activity of society. The plan identifies 10 areas which should be protected: information communication, finance, rail, air, electricity, gas, water, distribution, medical care and municipal services.

(5) RFID (Radio Frequency IDentification): ID tag with wireless communication capability

(6) *MULTI-S01* (MULTImedia encryption algorithm and Stream cipher No.01): A stream cipher operation mode developed by Hitachi in 2000. Conventional stream ciphers only provided a function for data confidentiality but with *MULTI-S01*, data tampering detection was also achieved. *MULTI-S01* was adopted as an ISO/IEC standard in July 2005.

(7) *MUGI* (MUlti GIga cipher): A stream cipher developed by Hitachi in 2001. *MUGI* was listed as a recommended encryption code for electronic government, and adopted as an ISO/IEC standard in July 2005.

(8) *HIME(R)* (High Performance Modular-squaring-based public-key Encryption): A public key encryption scheme, i.e. data is encrypted and decrypted using different keys, developed by Hitachi in 2001. *HIME(R)* was adopted as an ISO/IEC standard in May 2006.

■ Details of *Enocoro*

The *Enocoro* stream cipher family consists of two algorithms, *Enocoro-80* which has a key length of 80 bits and *Enocoro-128v2* which has a key length of 128 bits. *Enocoro*, based on the high-speed stream cipher *MUGI*, an ISO/IEC standard, achieves its reduced hardware circuit size by drastically reducing the number of registers required to maintain the internal state. Further, by employing the mixing function of the 2 iterations of SPN(9) structure, it is able to mix data on the register more efficiently, thus improving security at the same time as reducing power consumption.

Specifically, when *Enocoro-128v2* with a key length or 128 bits is compared with the light-weight implemented AES-128 which offers the same level of security, 2 to 10 times faster processing speeds were achieved, i.e. data encryption was achieved with even less processing. Further, when a field programmable gate array (FPGA) was used to measure the power consumption for encryption per bit: with AES it was 1.16 nano-watts per second (nWs), and with *Enocoro-128 v2* it was 0.103 nWs, confirming that Enocoro-128v2 consumed approximately one-tenth the amount of power to encrypt the same amount of data.(10)

(9) Substitution-permutation Network (SPN): A mixing method, also used in AES, where text replacement based on a substitution box and linear transformations are alternately repeated. MUGI employs a mixing method based on the Feistel scheme, and is comprised of a layer of the Feistel scheme. The Feistel scheme is also a mixing method, used widely in symmetric-key cryptography such as DES, which was standardized by the US in 1977.

(10) In practice, measurement results may differ depending on evaluation conditions.

About Hitachi, Ltd.

Hitachi, Ltd. (TSE: 6501), headquartered in Tokyo, Japan, is a leading global electronics company with approximately 320,000 employees worldwide. Fiscal 2011 (ended March 31, 2012) consolidated revenues totaled 9,665 billion yen ($117.8 billion). Hitachi is focusing more than ever on the Social Innovation Business, which includes information and telecommunication systems, power systems, industrial, transportation and urban development systems, as well as the sophisticated materials and key devices that support them.

For more information on Hitachi, please visit the company's website at http://www.hitachi.com.

# # #

Information contained in this news release is current as of the date of the press announcement, but may be subject to change without prior notice.
