FOR IMMEDIATE RELEASE

Successful development of biometric digital signature technology

- Achieving the same functionality as PKI without a smart card or password -

Tokyo, February 18, 2013 - Hitachi, Ltd. (TSE:6501, "Hitachi") today announced the development of provably secure digital signature technology based on the use of biometric information such as finger vein pattern in creating the signature. Through this, it will be possible to achieve an information security platform with the same functionality as the standard public key infrastructure(1) ("PKI"), based on individual biometric information without using a smart card or password. The technology will be developed as a convenient and secure digital signature technology along with applications such as in the national ID system, electronic government services, and electronic commerce. This work was supported by the Ministry of Internal Affairs and Communications, Japan.

In order to ensure the security of e-government, e-commerce and business information systems which have been increasing over recent years, it is imperative to prevent impersonation, document forgery or alternation. At present, PKI is widely used as the information security platform for this purpose. Digital signature technologies employed in PKI use a "secret key" to create a digital signature for an electronic document, and a "public key" to verify the signature to authenticate the creator of the document and prevent forgery and alteration. Currently, as the management of the secret key requires the use of a smart card or a password, it carries the risk of impersonation through theft or access loss due to losing the card or forgetting the password. If it were possible to use biometric information such as fingerprint, iris or finger vein pattern as the "secret key", then a smart card or password would become unnecessary, and an even more convenient and secure PKI could be achieved. Biometric information, however, is analog data which varies with environmental conditions such as lighting or temperature, or the person's physical condition, and therefore contains errors every time the data is captured. Until now, it was not possible to use a secret key which contained errors in digital signatures, and therefore biometric information has not been used.

To address this need, Hitachi has developed provably secure digital signature technology based on the use of information which contains errors, such as biometric information. Using the technology developed, it will be possible to employ individual biometric information without requiring a smart card or password, in achieving safe and secure systems for the national ID system, e-government or e-commerce.

This work was presented at the 30th Symposium on Cryptography and Information Security (SCIS 2013) held in Kyoto from the 22nd - 25th January 2013.

■ Details of the technology developed

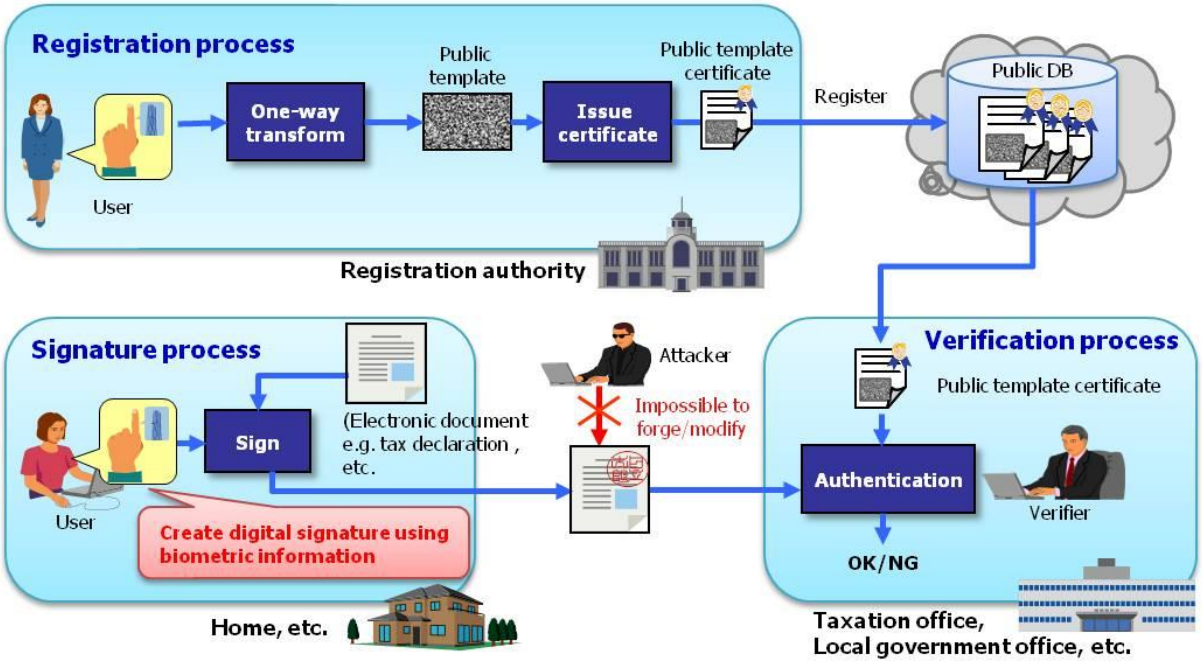
(1) Digital signature algorithm using biometric information as the secret key

In cryptographic technology for digital signatures or public key cryptography, as the secret key is processed as digital information, the key will be disabled if there is a difference in even 1 bit. In this work, technology was developed to enable the creation of a signature tolerating errors, and also, technology to correct the errors in the secret key in its secret form when verifying the signature. As a result, it is now possible to create a signature using a secret key with errors, and to verify the signature tolerating the errors.

(2) Mathematical verification of security

The security of this digital signature scheme developed by Hitachi can be proved by reducing it to the security of the Waters Signature[(2)] scheme. It was shown that if the method developed can be broken, then it will also be possible to break the Waters Signature. As the security of the Waters Signature has already been mathematically proven, the security of the method developed is also proven.

■ **Outline of the digital signature process using biometric information** (Overview of the biometric authentication public template platform)



(1) Public key infrastructure (PKI): An information security platform based on public key cryptosystems providing functions such as authentication, digital signature, and encryption.

(2) Waters Signatures: A digital signature scheme proposed by Brent Waters in 2005. Waters Signature has been shown to fulfill the requirements of EUF-CMA (probability of existentially unforgeable under chosen-message attacks), a widely accepted definition of the security of electronic signature schemes.

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 totalled 9,665 billion yen. 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.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.
