

SECURITY MANAGEMENT OF GENETIC INFORMATION USING STR PERSONAL IDENTIFICATION

Yukio Itakura^{1,2} Ph.D., Toshio Nagashima², Masaki Hasiyada³ and Shigeo Tsuji¹ Ph.D.

¹*Chuo University, Research and Development Center, Tokyo, Japan*

²*NTT Data Technology Corporation, Tokyo, Japan*

³*Tohoku University Graduate School of Medicine, Japan*



The ethical guideline concept announced by the Japanese Ministry of Health, Labor and Welfare in March 2001, contains seven basic elements and specifies that: a person's informed consent must be obtained before his/her DNA information can be collected and handled; that the human rights of the donor must be respected; and that procedures and facilities for strictly managing personal information must be established.

Taking into account the progress in research related to genetic-information decoding and the implementation of ethical guidelines for handling such information, this paper proposes a method for security management of genetic information using STR personal identifier and cryptography technology.

The operations of the genetic information security management system are:

(1) Public-key generation and registration

A public key is created using the algorithm using STR personal identifier. It is recorded in an IC card. Note that the person's DNA information is embedded in this public key.

(2) Collection of genetic information from an individual

The individual's consent must be obtained before his/her genetic information can be collected or transferred to related institutions. The system proposed in this paper leaves a consent signature as proof. To ensure that this system will work, it must be illegal "to handle personal genetic information not bearing a signature."

Next, the following security-enhancing functions can be added to the collection procedure:

- Personal authentication at the time of collection

At the time of collection, genetic information, as well as STR information for identification, is collected from the individual's DNA sample. This personal identification information is used as the basis for generating a public key. If the public key in the IC card presented by the individual can be generated from the personal identification information collected here, the collecting personnel can confirm that the individual is the legitimate owner of the IC card.

- Encryption of the collected information

When recording/storing an individual's genetic information, the medical institution encrypts it using the individual's public key. Decryption requires the IC card containing the individual's secret key. Even the individual's doctor is not allowed to check his/her genetic information without the individual's consent.

(3) Genetic-information transfer to related institutions and treatment-method inquiry

An inquiry about treatment methods can be sent to higher order institutions, such as general medical institutions or university research laboratories, by sending the individual's genetic information. Also, a pharmaceutical inquiry can be made by sending similar information to a pharmaceutical maker. Information transfer is conducted after encrypting the information based on the public key encryption method.