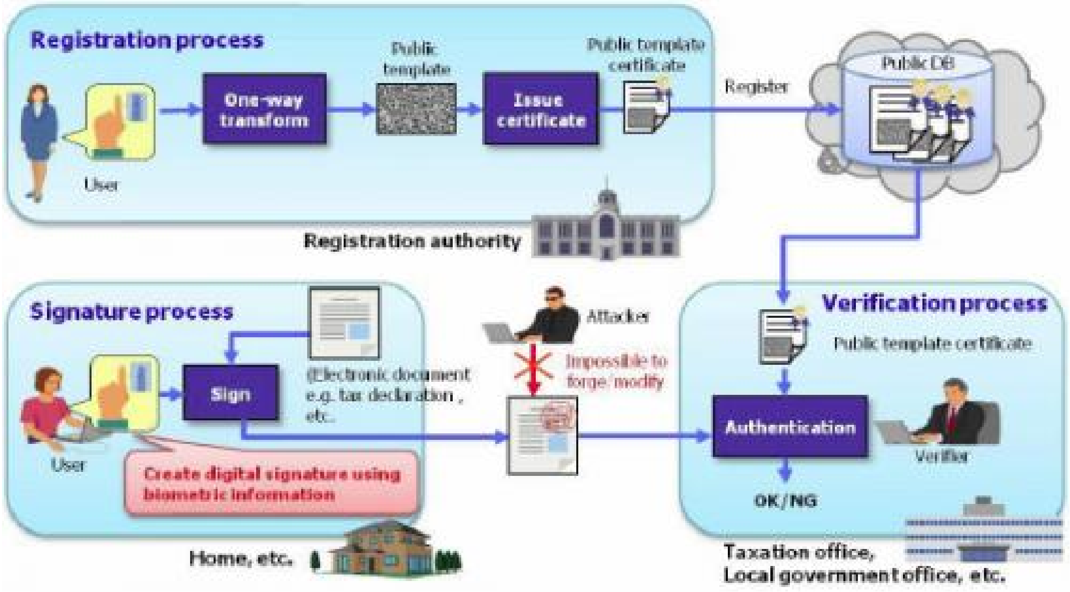
Successful development of biometric digital signature technology: Same functionality as PKI without smart card, password

February 26 2013



Hitachi, Ltd. recently 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 ("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.

Provided by Hitachi

Citation: Successful development of biometric digital signature technology: Same functionality as PKI without smart card, password (2013, February 26) retrieved 26 April 2024 from https://phys.org/news/2013-02-successful-biometric-digital-signature-technology.html