A STUDY ON THE STANDARDS OF THE MANAGEMENT OF SEGREGATED BIOMETRIC DATA

Yougjae Kim

Department of Business Administration, Korea Polytechnic University, Prof. ph.D.
Republic of Korea

ABSTRACT

This proposal of paper is the first international standard and research of the management technology of biometric data. By introducing and applying this international standards, everyone can acknowledge and approve are process for management of segregated biometric information. First, Safety requirement of segregated biometric information. Second, Growth and development of segregated biometric information. Third, Convenience promotion of financial transactions.

The demand for biometric authentication service is on a trend of significant increase owing to the advances in new technology such as the Internet of Things (IoT), artificial intelligence and others as well as the expanded use of fin-tech and electronic financing arrangements.

Biometric information is convenient because it is inherent and does not need to be remembered or stored, but leakage or misuse of the information could bring about serious problems because of its unique property. It is becoming more and more important to manage the information safely without the possibility of misuse or leakage. To store the information safely, it is effective to segregate the information into fragments in an un-usable form. Accordingly, we propose to standardize the international standard for Management of Segregated Biometric Information.

The purpose of paper is to propose to standardize the international standard of the distributed management technology of biometric data such as ISO, IEC, ITU and UNCEFACT

KEYWORDS

Management of Segregated Biometric Information, The Internet of Things, Artificial Intelligence, Biometric Information, Registration & Authentication Process

1. INTRODUCTION

This standard consists of the terminology, management and authentication processes needed to manage segregated biometric information. The biometric information used includes all biometric recognition technology through physical characteristics which can create encrypted biometric information such as fingerprints, veins, iris, face, voice, brainwaves, and electrocardiogram, and behavioral characteristics such as keyboarding or typing (key strokes), lip movement, eye blinking, walking, and hand gestures. This standard does not limit the types of biometric information and the precision of recognition of biometric information shall be considered by financial service providers when applying it to financial services.

The proposed paper specifies in its scope the framework and process for management of segregated biometric information, including the definitions and terms, the management process and the authentication process.

First, the definitions and terms.

Second, the management process of segregated biometric information. Such as,

· Registration, deletion, inquiry and renewal process of segregated biometric information

Third, the authentication process of segregated biometric information.

· Financial Institution Server Method(Proprietary authentication tasks)

· Segregation Management Center Server Method(Commissioned Authentication Tasks)

2. THE PURPOSE AND SCOPE OF THIS PAPER

2.1. The scope of paper

The objective of this paper is to help users by providing a way of the standardization and distribution of the International standards for the authentication method to verify the customers in non-face-to-face transactions by utilizing the biometric data registered by the customers split to and stored at multiple institutions for distributed management, the contributions can be made to the proactive response to the leakage of biometric data, prevention of the infringement of customer privacy and the activation of the biometric authentication and its related industries.

The scope of paper specifies a framework and process for management of segregated biometric information, including definition, management process of registration and authentication, deletion process, authentication module and distribute management of segregated biometric information.

First, Registration process of segregated biometric information.

Second, Authentication process of segregated biometric information.

· Financial Institution Server Method (Proprietary Authentication Tasks)

· Segregation management center Server Method (Commissioned Authentication Tasks)

Third, Deletion process of segregated biometric information

Fourth, Authentication module of segregated biometric information

Fifth, Distribution management of segregated biometric information

3. PREVIOUS STUDIES

The earlier study analyzed the previous studies and current state of international standards refers to the following latest versions

Table 1. Current state of international standards

Standard establishment organization	Standards name	Remarks
ISO/TC68 SC2	ISO 19092, Biometrics Security framework	Biometrics Application service
ISO/IEC JTC1 SC27	ISO/IEC 19790, Security requirements for cryptographic modules	
	ISO/IEC 24745, Biometric information protection	
	ISO/IEC 19792, Security evaluation of biometrics	
ISO/IEC JTC1 SC37	ISO/IEC 19784, Biometric application programming interface - Part 1: BioAPI specification - Part 2: Biometric archive function provider interface	
ITU-T SG17	ITU-T X.1086, A guideline to technical and managerial countermeasures for biometric data security	
KATS(Korea Agency for Technology and Standards)	KS X ISO/IEC TR 24722, biometrics – multi modal and – multi biometrics fusion	
	KS X ISO/IEC TR 24741, information technology –, biometrics tutorial	

4. THE REGISTRATION AND AUTHENTICATION PROCESS FOR MANAGEMENT OF SEGREGATED BIOMETRIC INFORMATION

The registration and authentication Process consist of fifth process for management of segregated biometric information such as the scope of paper and previous studies.

First. Registration process of biometric information

Second. Authentication process of biometric information

Financial institution server method (Proprietary authentication tasks)

Segregation management center server method (Commissioned authentication tasks)

Third. Deletion process of segregated biometric information

Fourth. Authentication module of segregated biometric information

Fifth. Distribution management of segregated biometric information

4.1. Registration Process of Biometric Information

· The registration template fragments are managed by the financial company and segregation management center in a distributed way.

· By splitting the biometric data into the fragments, to preclude the possibility of authentication, to be kept at different institutions for distributed management, the risks related to the hacking of information can be prevented

4.2. Authentication Process of Biometric Information

First, Financial Institution Server Method (proprietary Authentication Tasks)

· After establishing the proprietary authentication system, the financial company conducts the consolidation and authentication for the biometric data with segregation management center assuming the role for storing the fragments of the biometric data

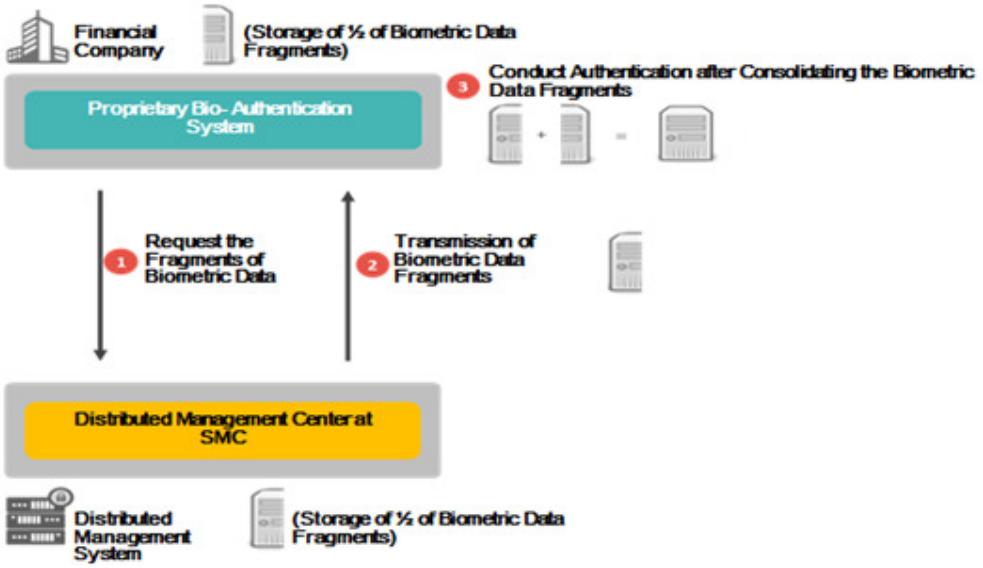

fig 1. Authentication Process

Second, Segregation management center Server Method (Commissioned Authentication Tasks)

· The financial company conducts the bio-authentication by using the shared authentication system offered by segregation management center, which assumes the role for consolidation and authentication of the biometric data.

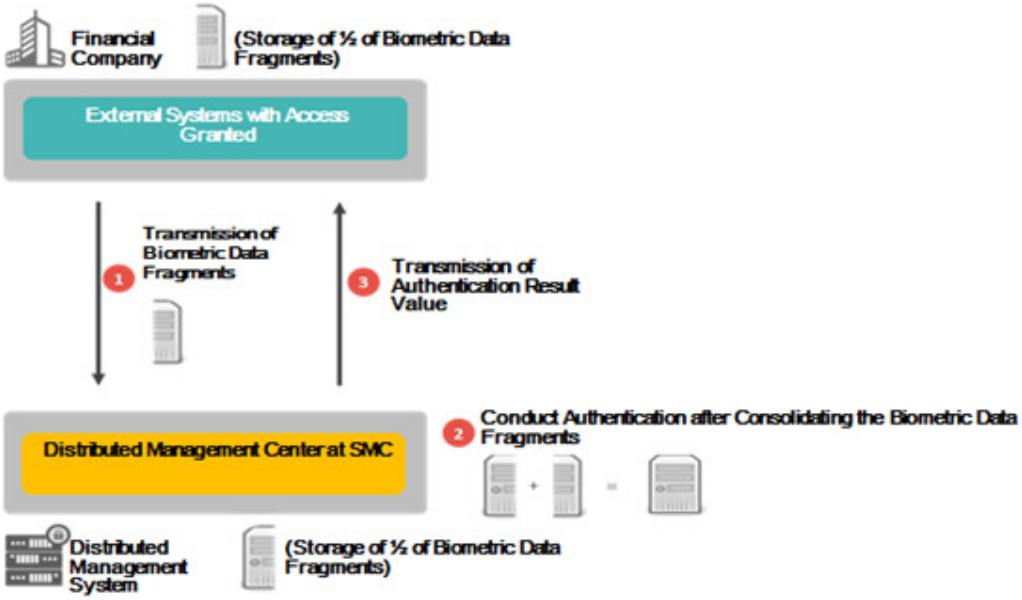

fig 2. Authentic

5. EXPECTED EFFECT

First, the activation of biometric authentication as well as the development of the related markets and industries can be pursued by assuring the compatibility and security of the technology for distributed management of biometric data.

Second, Enhancement of the possibility of overseas transplant of the domestic model for distributed management of biometric data.

Third, Assurance of the initiatives in related discussions and preparation of the foothold for preoccupancy of the markets through the pre-emptive development of the related international standards in the global Fin-Tech and security markets. The expected effects of this paper are summarized in Table 1.

Table 1. The expected effects of this Paper

	Benefits/impacts	Examples of organizations /companies to be contacted
Industry and commerce — large industry	All large industry (Financial transaction, e-Banking, Fintech, security, e-Payment & settlement)	Private company (Financial transaction, e-Banking, Fintech, security, e-Payment & settlement)
Industry and commerce — *SMEs	All SMEs (Financial transaction, e-Banking, Fintech, security, e-Payment & settlement)	Private company (Financial transaction, e-Banking, Fintech, security, e-Payment & settlement)
Government	Public area	Standard application business area
Consumers	End user	End user
Labour	Be increased in SME	Be reduced by apply standards and standards application
Academic & research Bodies	All academic & research bodies	All standard application business
Standards application businesses	All industry (Financial transaction, e-Banking, Fintech, security, e-Payment & settlement)	Underdevelopment industries

6. CONCLUSION

This study of the implications and significance intends to draw its conclusion as follows.

First, the demand for the biometric authentication is increasing significantly owing to the advance in new technology such as the Internet of Things (IoT), artificial intelligence and others and the expanded use of Fin –Teck, and electronic financing.

Second, biometric information is a unique characteristic to identify individuals, such as fingerprints, faces, veins and irises, that is used for authentication in a wide range of fields such as financial transactions, e-banking, fin-tech, e-Business, distribution industry and etc. Biometric information is convenient because it is inherent and does not need to be remembered or stored, but leakage or misuse of the information could bring about serious problems because of its unique property. It is becoming more and more important to manage the information safely without the possibility of misuse or leakage. To store the information safely, it is effective to segregate the information into fragments in an un-usable form.

Third, by ensuring the safety of the biometric information stored in a distributed way, the financial institutions are not allowed to infer the sound biometric information of customers and the fragmented biometric information is not available for use even if the fragments are leaked.

Fourth, The developed framework of standard of distributed management technology of biometric data guide the international law, rule and system of standard, technical regulation, conformity assessment, inspection, test and certification such as ISO, IEC and ITU standards and guideline.

Fifth, the convenience of the standard of distributed management technology of biometric data can be enhanced in financial transactions, e-banking, fin-tech, e-Business, distribution industry and etc.

REFERENCES

[1] A Study of biometric Approach Using Fingerprint Recognition Lecture Notes on Software Engineering, Vol.1 No.2 May 2013 Ravi Subban and dattatreya P.Mankame page 211-213

[2] Biometrics Management Guidelines for the finacial security,TTA(Telecommunications Technology Association) 2016.12.02

[3] Ensuring Quality in Biometric Systems Md. Mahbubur Rahman, Amit Karmaker, Md.Mahmudul Hasan, Samsuddin Ahmed international Journal of Security and Its Applications 2015 September Vol.9 No 4

[4] ISO 19092, Biometrics Security framework, ISO/TC 68 SC2, 2015

[5] ISO/IEC 24745, Biometric information protection, ISO/IECJTC1 SC27. 2015

[6] ISO/IEC 19792, Security evaluation of biometrics, ISO/IECJTC1 SC27. 2015

[7] ISO/IEC 19784, Biometric application programming interface, ISO/IEC JTC1 SC37.2015

[8] ITU-T X.1086, A guideline to technical and managerial countermeasures for biometric data security, ITU-T SG17

[9] Segregated management of biometric data information, Korea payment settlement association Park Jung Gook 2016.12.05

[10] Standard of segregated management biometric data, ISO/TC 68 SC2 Presentation, 2018.04.25

[11] "A novel way of ICON based authentication methods", Advance Computing Conference (IACC) 2015 IEEE International, P Devaki, Raghavendra Rao, pp. 449-453, 2015.

AUTHORS

Younjae Kim

Short Biography
ISO/IEC SC32 WG1 Vice Convenor
ISO TC 68(Financial Service)
Uncefact International Trade and Business Group Vice Convenor