A Study on FIDO Authentication System for Reinforcing the Security of Electronic Medical Records

Sujin Kim , Jinwoo Jung and Jungduk Kim

Security Convergence Department, Chung-Ang University, Seoul, Korea

Abstract. The target of compulsory certification in Information Security Management System has extended to medical institutions. This caused us to recognize the importance of information security in modern hospital information system that has changed from the medical record management that was recorded and managed largely in paper chart in the past to the Electronic Medical Record that medical personnel enter patient information into a computer directly for building a database. As medical institutions manage sensitive information like personal information basically, personal medical data infringement accident, if occurred can become a big social issue. Currently, the medical information in medical institutions are stored in electronic medical records and to access, user authentication is required by means of accredited certificate as security measure. Accredited certification has technical problems such as certificate storage method and security level of password and managerial problems such as certificate copy/leak/share. In this respect, this study proposes and presents how to build the FIDO-based authentication system that applies UAF or U2F authentication mechanism depending on the authority and work scope of medical personnel and medical support assistant like staffs, officers, licensed practical nurse and so on, within large medical institutions that use medical information system. The aim is to solve problems in accredited certificate authentication method in the existing medical institutions with the FIDO-based authentication system proposed in this study.

1 Introduction

Medical information management in medical institutions has changed from the medical record management that was recorded and managed largely in paper chart in the past to the Electronic Medical Record that medical personnel enter patient information into a computer directly for building a database. This caused people to keep raising the necessity of applying information security management method that was thought to be important in the existing companies and/or governmental agencies to medical institutions [1].

Information Security Management System authentication system is a system that screens information security management system that is established, operated, and managed to protect major information assets of companies and agencies from different kinds of threat [2]. Since medical institutions deal with sensitive information, especially health status, medical record, and other personal information, personal medical information infringement accident due to hacking, exposure to insider, malicious data leak and so on, can become a big social issue [3].

For this reason, the government revised the 'Act on Promotion of Information and Communications Network Utilization' in June to expand the target of compulsory certification in Information Security Management System authentication system to medical and educational fields. Thus a total of 43 large hospitals were included into the target of compulsory certification in Information Security Management System.

In line with this, medical institutions also tend to recognize the importance of information security. Currently, the medical information in medical institutions are managed through electronic medical records and as means for security authentication to access this, medical personnel use accredited certificate method. Medical institutions are using accredited certificate to acquire the legal force of digital signature and the reliability of records. Indeed, it has technical problems such as authentication certificate storage method and program installation and managerial problems such as certificate copy/leak/share [4].

This study provided the FIDO-based authentication system that applied UAF or U2F authentication mechanism depending on the authority and work scope of medical personnel and medical support assistant within large medical institutions, in other words, secondary and tertiary institutions that used the medical information system and proposed how to build such a system. This study aims to solve the problems of accredited certificate authentication method in the existing medical institutions by using the certification system proposed in this study.

2 Literature

2.1 Concept Range Setting of Electronic Medical Record and Medical Treatment Information

Electronic Medical Record (EMR) is a form that medical records recorded by the medium of paper are improved equally through computerization without any transformation of business transaction method, scope of information, and information content. In other words, it indicates a system that medical information such as business data, treatment, and surgery centering on patient treatment are input and stored into a computer [5].

The definition of medical information does not exist clearly in the current laws and regulations. In addition, most medical information do not have clear definitions and regulations although they recognize medical information as sensitive one. Instead, 'personal medical information' is used to indicate medical practice related information that medical personnel and medical treatment institutions use for the purpose of national health care and promotion in general and also understood as encompassing not only the data collected across the entire process of medical practice but also the information studied based on this [6].

This study defined the concepts of medical information that were not clearly defined as 'sensitive medical information' and 'universal medical information' by using the comprehensive concept of 'personal medical information' to identify and improve the problems in security of electronic medical records.

'Sensitive medical information' is defined as indicating the information that such medical personnel as doctor and nurse who treat patients among many health care providers for patients have access and use.

'Universal medical information' is defined as indicating the information that nurse assistants and individual responsible for medical support assistants who are in charge of office work and administration within medical institutions and do not engage in medical treatment have access and use for medical support assistant and business transaction purposes only, in other words, relatively less sensitive medical information rather than 'sensitive medical information.'

2.2 Authentication Certificate-based Certificate System Using Electronic Medical Records

In accessing the electronic medical records, one's identity is checked by verifying digital signature generated by using medical personnel's private key. If digital signature is done in accessing the electronic medical records, the system determines whether to approve or not by verifying the validity, status, and digital signature within the time limit of the accredited certificate [7].

However, authentication certificate-based authentication system has caused many inconveniences for medical institution users due to many other security limitations. Moreover, with the increasing number of various security related issues, there is a need to introduce a new certification system. The problems of the authentication certificate identified through previous related studies are analyzed in the table below.

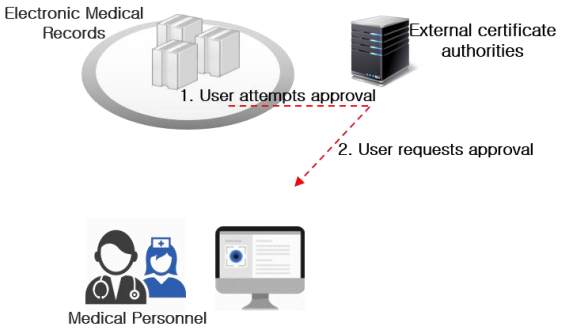

Figure 1. Authentication system based on PKI in medical institutions

Table 1. The problem of PKI based authentication system

Field	Item	Problems
Technical	Authentication certificate storage method	Authentication certificate is stored in non-standardized location (NPKI) where security is not secured[8]
	Certificate status check through external network	The validity of authentication certificate must be checked for every digital signature, but constraints still exist because EMR is a form of personal area network[9]
Managerial	Certificate duplication and leakage	As it is a form of file., anyone can copy and leak certificate private-key easily in the form of Cut & Paste even if it is not a security token[8]
	Password security level	Password that is made by using simple information or personal information that is easy to remember[9]
	Accredited certificate sharing	Vulnerable in managerial security as it is possible to share and use certificate without limitation in fact[10]

2.3 FIDO(Fast IDentity Online) Certification

FIDO is an abbreviation of Fast IDentity Online and indicates a technical standard of FIDO Alliance established in 2012 to support the safety, universality, and simplicity of user identity certification in online environment. FIDO Alliance enacted two standards: UAF, a certification mechanism by using individual user's unique biometric information and U2F, a certification mechanism to add secondary certification factor like security token including USB dongle that stores private key secondarily after getting an approval for the existing ID/password and announced on Dec., 2014.

The first certification mechanism is UAF(Universal Authentication Factor) and authenticates users by linking the authentication method provided in user's device with online service. UAF authentication procedure can be largely divided into twos: registration procedure that

authentication token and public key are registered into FIDO server by executing biometric authentication via individual user's device and using generated key pairs and authentication procedure that the challenge value and authentication token transmitted when user requests login to server are transmitted to server after signature by using the private key stored in user's device and the values are verified by using the private key within server[11].

Figure 2. FIDO UAF Authentication Process.

The second is U2F(Universal 2nd Factor) and adds token (e.g. USB dongle) that applies encryption-based security technology in the online service that uses the existing ID/password as two-factor authentication factor. It identifies user by using the security module like security token and protects authentication value safely from various malignant codes by directly communicating the result values certified through PIN with web browser[12][13].

In addition, what is different from the existing authentication method is that authentication procedure cannot be performed if U2F dongle is not owned when other's password was seized. The currently released U2F dongle includes biometric authentication function and so if biometric information-based user authentication is not performed through the sensor fixated to dongle in case of connecting USB, dongle is not activated.

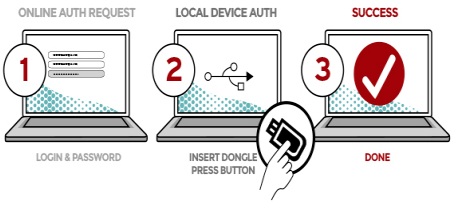

Figure 3. FIDO U2F Authentication Process.

The overall registration and authentication procedure of FIDO uses a public key-based encryption method similarly to the existing authentication certification system. However, the clear advantage of FIDO can be free from technical and managerial problems because it separates user verification from authentication process and uses biometric information when verifying user, but this biometric information is stored in user's device only without being stored and/or disperse-stored to server within service institutions like the existing Fast Identity Online. It is less likely to be abused because biometric authentication procedure must be preceded prior to FIDO server certification even if device was lost[14].

3 FIDO-based Authentication system

This study proposed a FIDO-based authentication system to improve the problems in the existing authentication system targeting large medical institutions.

3.1. FIDO-based Authentication System Electronic Medical Records System Building Plans in Large Medical Treatment-related Organization

In medical institutions, the FIDO-based authentication system building measure may depend on the size of medical institution, but this study selected large health organizations.

According to the Article 9 of the Medical Care Assistance Act, large medical institutions are considered as secondary if they hold over 30 nursing care beds and possess legal treatment department requirements and as tertiary if they hold over 500 nursing care beds and medical professionals for all treatment departments.
Such large medical institutions are recommended to build a FIDO authentication system separately and the specific measures are shown in the figure below.

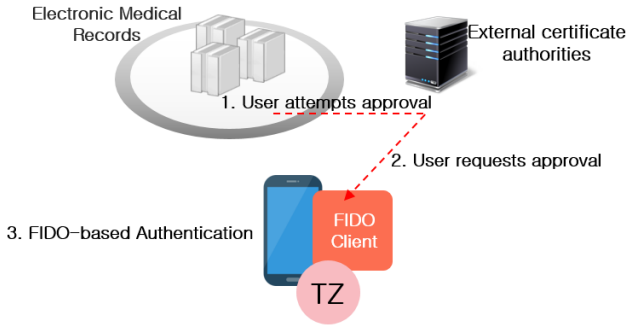

Figure 4. Proposed FIDO Authentication system.

The proposed FIDO authentication system applies public-key infrastructure (PKI), core technology of information security, performs digital signature within TZ(Trust Zone) safe against memory hacking to secure the reliability of user certification within various medical service environment, and supports strong security and non-repudiation against the existing authentication certificate environment.

It can also solve the problem of the present authentication certificate system, i.e. 'certificate check through external network' by locating FIDO authentication server within the personal area network. Given various environments and scales of domestic medical market, there are limitations in developing a PKI certification environment for medical purposes, and so building user certification system that observes the FIDO standards can be considered as reasonable measure[14].

3.2 FIDO-based Authentication System

Place the figure as close as possible after the point where it is first referenced in the text. If there is a large number

of figures and tables it might be necessary to place some before their text citation. If a figure or table is too large to fit into one column, it can be centred across both columns at the top or the bottom of the page.

2.1.1 U2F-type Authentication System

U2F-type Authentication System targets medical personnel who need to access sensitive medical information like a medical treatment information and performs two-factor authentication by using the U2F token to store security key in the manner that authentication device is not included in private device. So it is expected to have an effect to reinforce the managerial security.

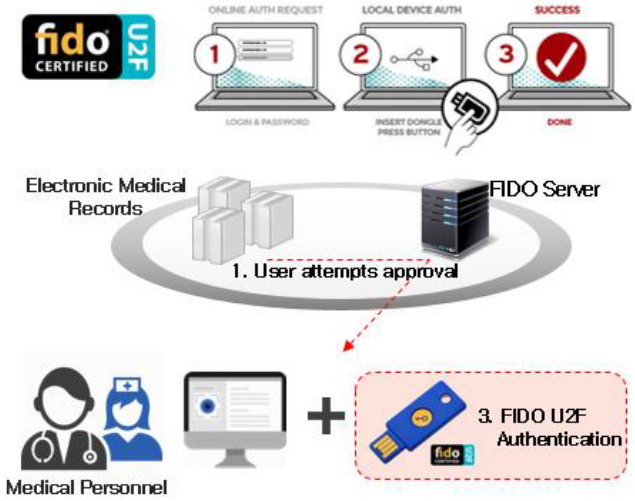

Figure 5. Proposed authentication system by FIDO U2F

If a medical personnel attempts approval to access sensitive medical information (treatment information), FIDO server requests user authentication to the medical personnel. Medical personnel perform FIDO authentication by using USB dongle that uses U2F after performing the existing ID/PW certification. This U2F dongle is attached with biometric certification sensor and the sensor is activated only by medical personnel who are approved or through biometric certification. This certification improves security by performing secondary certification with U2F dongle and at the same time clarifies accountability through biometric certification by using dongle.

2.1.2 UAF-type Authentication System

UAF-typed Authentication System targets medical institution employees including employees in the department of medical record and nursing assistant who need to access universal medical information(health information). The system uses the UAF-based biometric certification method that authentication device is included in private device and utilizes the mobile device into private device by considering rapid certification procedure and convenience, universality, and safety in access. The present FIDO 1.0 version is limited to mobile devices, but from the FIDO 2.0 version, FIDO UAF technology can be implemented in most devices like PC and tablet that are based on authentication through web.

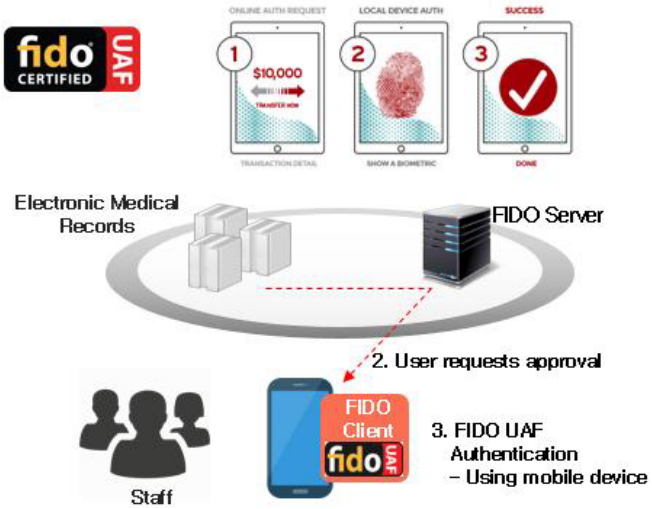

Figure 6. Proposed authentication system by FIDO UAF

If staff – employees in department of medical record and nursing assistant, and others – attempts approval for accessing the universal medical information (health information) rather than medical personnel within hospitals, FIDO server requests user approval to the staff. The staff performs biometric certification through personal device mounted with applications and FIDO clients and obtains certification from FIDO server if user identity is identified. As certification is proceeded by using the FIDO UAF-based private mobile devices, it provides immediacy, convenience, and universality. In addition, as certification is proceeded by using a personal device that is based on biometric certification, accountability can also be clarified.

4 Conclusion

The importance of medical data privacy protection has become an issue not only in laws and regulations but also in social dimensions. Currently, the medical information in medical institutions are computerized and stored in electronic medical records and accordingly for obtaining security and reliability, they use authentication certificate-based authentication system. However, the present authentication certificate-based authentication system has limitations in checking the status of authentication certificate by external network certificate authorities due to storage private key in places where security is not ensured, vulnerability in password security level in authentication certificate, and electronic medical records established in private networks. It also has managerial problems in that authentication certificate is easily copied and leaked because it is the form of a file and the non-repudiation is not valid actually as it shares the accredited certificate.

To solve these problems, this study proposed methods to introduce FIDO, the next-generation authentication system. FIDO-based authentication system uses public

key-based authentication like the existing authentication certificate-based authentication system, but user verification and certification are separately proceeded and the biometric information used in generating private key for verification is not stored separately in server and rather stored within device only, which may increase the private key security. Also, differentiating the authority and role to access medical information system by using the FIDO-based authentication system and applying different UAF and U2F technologies can support strong security and non-repudiation and clarify responsibilities against the existing authentication certificate system. Furthermore, implementing simpler and stronger alternate authentication technologies in combination with biometric certification can provide convenience in user service access.

Nevertheless, the proposed FIDO-based authentication system is the one that proposed FIDO 1.0 technical specification and FIDO1.0 has limitations in that certification can be proceeded only by mobile devices if UAF technology is applied. This can be improved by the FIDO 2.0 to be enacted at the end of this year.

So, further studies need to verify case studies and empirical ones that addressed the actual application of the FIDO-based authentication system in the proposed medical fields.

References

1. J. Lee, H. Jo, S. Park, Y. Gang, KIISC Review **23**, 34 (2013)
2. J. Kim, K. Lee, KIISC Review, **18**, 1 (2008)
3. Y. Jung, Y. Lee, Health and welfare policy forum, **205**, 70 (2013)
4. C. Jung*, University of Soongsil, Seoul*, (2012)
5. Y. Jeon, The korean journal of health service management, **7**, 224 (2013)
6. G. Jung, Journal of korea information law, **6**, 3 (2002)
7. M. Fritscher, *Fifth Americas Conference on Information Systems*, 432 (1999)
8. G. Kim, People and ideas, **181**, 163 (2013)
9. Y. Lee, The KIPS transactionsty C, **18**, 379 (2011)
10. A. Salaiwarakul, M. Ryan, *IWSEC*, 231 (2008)
11. S. Kim, The Journal of The Korean Institute of Communication Sciences, **33**, 59 (2016)
12. FIDO Alliance, Universal 2nd Factor (U2F) Overview, 2015
13. FIDO Alliance, FIDO 1.0 Final Specifications have arrived, 2014
14. K. Lee, ICT standard & certification TTA journal, **165**, 12 (2016)