International Journal of Engineering & Technology, 7 (2.33) (2018) 41-44

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

The framework of user information protection via secure SSO and PKI

Jeong Oh Kim [1] *, Min Woo Park [1], Woo Seung Jo [1], Ki-Seok Choi [1]

[1] NTIS Center, 245, Daehak-ro, Yuseong Gu, Daejeon, 34141 South Korea
**Corresponding author E-mail: jokim@kisti.re.kr*

Abstract

Background/Objectives: There has been a necessity of a new system to protect and share user information with cooperative research institutes and manage subjects for managing and providing national R&D information.
Methods/Statistical analysis: The National Science & Technology Information Service (NTIS) used the SSO API to share user information with cooperative research institutes safely. The API included minimum information only to prevent personal information such as user ID and authorization code from being leaked and observed related laws. For the authorization and management of user information targeted to open R&D information, moreover, 2-stage authentication has been established, using the certificate authentication system.
Findings: Since information is collected and provided in diverse manners by multiple institutes, user information has been scattered, and there has been a risk of the leak of personal information. With the centralized collection and management of user information, however, the protection of personal information and observance of laws have become more convenient. Furthermore, the information is provided to the authorized managers only through the construction of a security system and utilization of access control system, and security has been secured. To make users utilize information properly at access to raw data, authorization procedures were strengthened, keeping national R&D information and users more reliable.
Improvements/Applications: Through this framework, secure information-sharing & management systems were applied, improving the safety of information management.

Keywords: *National R&D Information; NTIS; User Information Management; Single-Sign on; Public Key Infrastructure*

1. Introduction

The NTIS is the first national R&D information knowledge portal service which collects, processes and spreads national R&D information (e.g., Program, project, personnel, outcome, equipment & facilities, etc.) throughout the life cycle of national R&D programs [1-3]. For the collection and processing of the information scattered across 17 government bureaus and offices, 422 standard items were enacted and amended to establish an efficient management system. In addition, national R&D information from each government unit are collected and managed automatically or via the online registration system "National R&D Standard Information Management System". To keep the information stable with such government bureaus and offices, there have been diverse studies such as the construction of standard linkage platform4. To establish and provide highly useful services by analyzing the information collected through linkage and registration according to its characteristics and purposes, a system in which a cooperative study is performed by four agencies has been developed. However, personnel (researcher) information among such national R&D information is collected by the KISTI in an integrated fashion and used by cooperative research institutes. Under these policies, it was needed for cooperative research institutes to share personnel information. In other words, there was a necessity to design a system to share personnel information by observing the related laws (e.g., Regulations such as Personal Information Protection Act, etc.) and regulations (e.g., Information Security & Personal Information Protection Guideline, etc.).

Recently, there have been a lot of interests in 'information' such as big data, open science, artificial intelligence and 4th industrial revolution. At the same time, there has been a rising demand for highly reliable information and standard information [5-6]. A demand for national R&D information has continuously increased as well. Under 'Government 3.0' as well, the data created by the government were disclosed, or those produced with government budget were open to the public [7-8]. Therefore, the NTIS also attempted to provide national R&D information to more users by developing a policy to expand the opening of national R&D information. The agency has developed systems, policies to expand the opening of national R&D information through diverse methods such as NTIS cloud, national R&D disclosure (one-stop information sharing), and search result download [9-10]. In particular, as the scope of information provided increased from 28% to 70% through search result download and opening of national R&D information, there was a necessity to strengthen information protection and verification procedures. In addition, a process to provide unified information to cooperative research institutes has been established to provide information. To provide the information which has been provided under different management systems in a safe and effective manner, however, a new system which ensures the safe management and use of user information is essential.

To provide organic NTIS services together with four cooperative research institutes, this study observes the information security and personal information protection system according to the necessity of building a researcher-information sharing system, open science and a policy to expand the opening of open science and

national R&D information, implies a necessity to build an environment to provide national R&D information safely and constructs a framework and security system accordingly. Specifically, this study suggests a user information protection and safe use system by constructing a user information management framework using Single-Sign ON (SSO) with cooperative research institutes and through the NPKI-based user authentication system to keep the provision of information stable according to the opening of information. Furthermore, this study explains what environments and specific plans are needed for the NTIS to provide such methods.

2. Materials and methods

For the management of national R&D information and expansion of its opening, the NTIS has attempted to collect and provide national R&D information in accordance with the related laws (e.g., Personal Information Protection Act, etc.) and regulations and 'Government 3.0'. Then, this study designs and proposes a user information management framework. Furthermore, it targets to keep the user information secure through the construction of physical and managerial security systems including SSO and PKI.

2.1. User information management with cooperative institutes using SSO API

For the management of national R&D information with cooperative research institutes and provision of the NTIS services efficiently, the roles were classified according to the characteristics of each agency and information. Table 1 below states the information usually managed by each institute. The KISTEP manages project/program information and information linkage & collection while the KISTI handles project/research/performance information and science & technology equipment and facility information. In addition, the KBSI controls research equipment & facility information. In case of project information, especially, it is classified into investigation & analysis information and realtime collection information, and there is difference in the purpose of the use. Therefore, it is collected and managed by both the KISTEP (investigation & analysis) and KISTI (information collection). The researcher and facility-related information needed to perform projects and programs and research outcome information from the projects are correlated with each other systematically. The research outcome from each project/program would be used to create a new project/program.

Regarding the collected national R&D information, the requirements and standards of the information that users can approach differ. In order for the NTIS service user to get access to such information, therefore, access authority should be granted by each authority. In addition, there was a necessity to develop verification procedures and policies to check if the information can be properly used. Therefore, it was needed to build a system through which information can be approached, using user information. The system in which authority is granted individually by each agency is inefficient so that there was a necessity to build a system for the integrated management of information.

Table 1: Managing Institute of Characteristic of Information

Characteristic of Information	Institute
Program	KISTEP
Project	KISTI/KISTEP
Researcher	KISTI
Equipment	KBSI
Outcome	KISTI

To share and manage user information safely with cooperative research institutes, this study designed a SSO-based user information management framework. The SSO server which manages user information was separately constructed from other servers to ensure security. For network security, furthermore, positive regulation-based IT/port access control and IPS/web firewall/firewall were applied. Furthermore, API was provided to have user information (ID, authority information) checked and verified through the SSO.

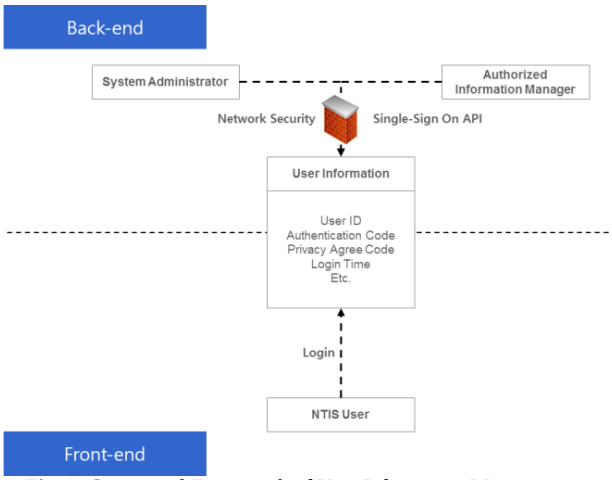

Fig. 1: Conceptual Framework of User Information Management.

Figure 1 above illustrates a conceptual framework regarding users' information access. Once a user logs in, user information is packaged to have the information (e.g., user ID, authority code, consent to hold personal information, local/foreigner code, login time, etc.) managed through the SSO. The system administrator and authorized information manager (service manager) construct and operate the NTIS services based on the SSO API according to the access control policy under the network security control.

2.2. User information authentication based on national PKI

According the policy to expand the opening of national R&D information (28% 70%, NTIS cloud); the scope of access to the information provided by the NTIS has increased. As more information became approachable, definition on user scope and subject of punishment were also decided by policy. Since the NTIS cloud targets to support the national R&D information inquiry & analysis functions, conventional operating policies were kept as they were. In case of newly expanded search result download or opening of raw national R&D information, however, there was a necessity to apply a user authentication system through local/foreigner classification and PKI for the proper utilization of national R&D information and prevention of its illegal leakage. In addition, minimum information was provided to non-members just like foreigners, and it was basically kept secure. As such open item and subject-related policies were confirmed, there was a demand for a plan to build a new system for user management.

Table 2: User Information via SSO for Sharing the Cooperate Institute

Traditional SSO	Advanced SSO for Information disclosure
	User ID
User ID	Authentication Code
Authentication Code	Privacy Agree Code
Privacy Agree Code	Login Time
Login Time	Identity Verification Code
	Domestic/Foreign Code

Table 2 above states conventional SSO and new SSO which would be revised according to the opening of national R&D. To clarify user authentication and local/foreigner classification, mobile phone/i-PIN authentication procedures were added to the SSO API-based user information. Furthermore, a code which performs user authentication against the locals was added. Figure 2 shows user verification procedures when a user logs in to get raw national R&D information. If login is attempted, whether or not user authentication is already conducted is checked. Unless a user's identify is confirmed, a user authentication procedure should be performed. Once user authentication is confirmed, the information

needed for the automatic logout of the NTIS services and access record storage is added to user information in Figure 1, and the related information is encoded. Then, the second authentication procedure is carried out. Before this PKI authentication, local/foreigner is classified. If confirmed as 'Local', the PKI authentication is performed, and raw national R&D information is provided.

Algorithm Login via SSO
Step 1. Check identity verification
if (verification code is false)
Request identity verification
Step 2. Add user IP, timestamp to user information
Step 3. Encode whole information
Step 4. /* Verify using National PKI authentication */
Check domestic/foreign code
if(code is true)
Request PKI authentication
Provide national R&D information

Fig. 2: Pseudo-Code of User Login with Verifying the Authentication.

3. Results and discussion

For the efficient management and use & spread of national R&D information, this study constructed a system which manages and authenticates user information. For the efficient management of information, users were classified (e.g., chief research officer, bureau, project management institute, etc.), and authority was added to the SSO API. Figure 3 below shows a list of the authorities used for each agency to manage user authority. The related information such as ID and authority information by access system (e.g., authority code, term of authority) was added to the SSO API, and it was checkable by each manager. As shown in the figure, diverse management systems are shown without agency classification. However, the information managers from each institute are able to search the authority of the services which are currently under control. In addition, a user verification procedure for the opening of raw national R&D information was established. Figure 4 below reveals the information provided to the users who didn't complete user authentication. They are required to enter local/foreigner classification, department and user type. Then, they are classified by local/foreigner, department and user type. After that, mobile phone / i-PIN authentication is performed. There also was an additional authentication procedure to find out if local/foreigner and user verification were properly carried out.

권한현황 | [총 20082 건]

	아이디	성명	소속기관	시스템	사용자권한	권한사용기간	요청일자	승인상태
☐	jhj•••	장*환	한국기계•••••••	국가R&D표준정보관리서비스	연구책임자	2017- ~ 2018-	2017-	승인
☐	ckd•••••••	여*환	한국건설•••••••	국가R&D표준정보관리서비스	연구책임자	2017- ~ 2018-	2017-	승인
☐	hsh•••	홍*호	한국화재•••••••	국가R&D표준정보관리서비스	연구책임자	2017- ~ 2018-	2017-	승인
☐	ksp•••••••	신*우	국민체육•••••••	연력종합관리시스템(평가위원)	과제관리기관담당자	2017- ~ 2018-	2017-	승인
☐	KIM•••••••	김*형	경민대•••••••	국가R&D표준정보관리서비스	연구책임자	2017- ~ 2018-	2017-	승인
☐	lcw•••	이*우	숭실사이버•••••••	국가R&D표준정보관리서비스	연구책임자	2017- ~ 2018-	2017-	승인
☐	wor•••	박*혁	한국철도•••••••	국가R&D표준정보관리서비스	연구책임자	2017- ~ 2018-	2017-	승인
☐	was•••••••	남*군	한국소방•••••••	국가R&D표준정보관리서비스	연구책임자	2017- ~ 2018-	2017-	승인
☐	che•••••••	황*홍	대전대•••••••	국가R&D표준정보관리서비스	연구책임자	2017- ~ 2018-	2017-	승인
☐	pir•••••••	백*현	한국보건•••••••	사업관리서비스	과제관리기관/부처	2017- ~ 2019-	2017-	승인

Fig. 3: The List of Authentication Management.

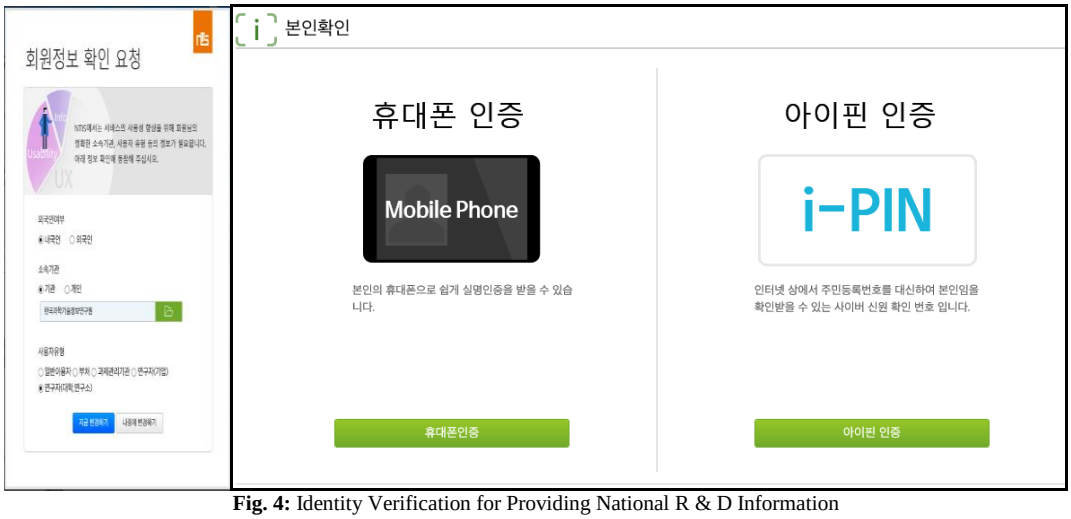

Fig. 4: Identity Verification for Providing National R & D Information

When raw national R&D information is provided through the R&D open services, user authentication is performed through PKI. Unlike search result download and NTIS cloud, the target of the opening of raw information through the R&D open services was limited to public organizations. Therefore, the GPKI was used. When a user from the public agencies which do not have GPKI wants to get the raw data, he/she was required to go through user authentication through his/her employment certificate.

The user management framework designed to manage and provide national R&D information should be continuously upgraded to

prevent the leak of personal information through the improvement of security and continued information control. In addition, it is needed to consider the additional application of one-time password (OTP) to share user information and strengthen user authentication using a private network such as Virtual Private Network (VPN). In addition, the improvement of user convenience by expanding user access to R&D open services and application of general PKI would also be a critical implication.

4. Conclusion

This study proposed a method to construct a user information management & sharing framework to protect personal information and keep it secure and described the results of its application. In terms of security, authorized information managers are only permitted to approach the SSO API through security system and access control. For the protection of personal information, in addition, minimum user information was shared through the SSO API. To provide national R&D information in a safe and secure fashion, furthermore, user information authentication procedure was added. To make national R&D information properly used through user verification/PKI-based user authentication, user management procedures were reinforced. Even though both efficient management and security were ensured, continued management is needed.

5. Acknowledgment

This research was supported by Maximize the Value of National Science and Technology by Strengthen Sharing/Collaboration of National R&D Information funded by the Korea Institute of Science and Technology Information (KISTI).

References

[1] TH Kim, WK Joo, MS Yang, DY Nam, P Kim, KS Choi, Integrated R&D Information Service System of the Contributed Research Institues, Proceedings of the Korea Information Processing Society Conference, 2005, 1(1), pp. 121-124.

[2] MI Kim, SJ Jhun, BJ You, A Study on a Method to Construct a System for Sharing National R&D Information, Proceedings of the Korea Contents Association Conference, 2006, 10 (1), pp. 698-701.

[3] National Science & Technology Information Service, http://www.ntis.go.kr.

[4] HS Choi, JS Kim, Desing of a NTIS Information Integration Model based on a Standard Integration Platform. Journal of KIISE, 2012, 18(6), pp.484-488.

[5] Nancy P, Petr K, Matteo C, Samuel P, Fostering Open Science to Research using a Taxonomy and eLearning Portal, i-KNOW '15 Proceedings of the 15th International Conference on Knowledge Technologies and Data-driven Business, 2015, 11 (1), pp. 1-8.

[6] Peter M-R, Open data in science, Serials Review, 2008, 34(1), pp. 52-64.

[7] KOREA Government 3.0, http://www.gov30.go.kr.

[8] Open Data Portal, http://www.data.go.kr.

[9] MI Kim, SJ Jhun, BJ You, A Study on a Method to Construct a System for Sharing National R&D Information, Proceedings of the Korea Contents Association Conference, 2006, 10(1), pp. 698-701.

[10] MW Park, NG Kang, MS Yang, KN Choi, A Study of Cloud-based Analysis Platform for Sharing and Disclosure of National R&D Information, International Journal of Applied Engineering Research, 2015, 10(90), pp. 844-847.