九州大学学術情報リポジトリ
Kyushu University Institutional Repository

Introduction of Unchanging Student User ID for Intra-Institutional Information Service

Kasahara, Yoshiaki
Research Institute for Information Technology, Kyushu University : Assistant Professor

Fujimura, Naomi
Faculty of Design, Kyushu University : Professor

Ito, Eisuke
Research Institute for Information Technology, Kyushu University : Associate Professor

Obana, Masahiro
Information Technology Infrastructure Division, Information System Department, Kyushu University

https://hdl.handle.net/2324/1563581

出版情報：Proceedings of the 2015 ACM Annual Conference on SIGUCCS, pp.141-144, 2015-11-09. ACM
バージョン：
権利関係：

Introduction of Unchanging Student User ID for Intra-Institutional Information Service

Yoshiaki Kasahara
Kyushu University
6-10-1 Hakozaki, Higashi-ku
Fukuoka 812-8581, Japan
+81 92 642 2297
kasahara.yoshiaki.820@m.kyushu-u.ac.jp

Eisuke Ito
Kyushu University
6-10-1 Hakozaki, Higashi-ku
Fukuoka 812-8581, Japan
+81 92 642 4037
ito.eisuke.523@m.kyushu-u.ac.jp

Naomi Fujimura
Kyushu University
4-9-1 Shiobaru, Minami-ku
Fukuoka, Japan
+81 92 553 4434
fujimura.naomi.274@m.kyushu-u.ac.jp

Masahiro Obana
Kyushu University
6-10-1 Hakozaki, Higashi-ku
Fukuoka 812-8581, Japan
+81 92 642 7654
obana.masahiro.049@m.kyushu-u.ac.jp

ABSTRACT
In Kyushu University, a traditional "Student ID" based on student number assigned by Student Affairs Department had been used as the user ID of various IT services for a long time. There were some security and usability concerns using Student ID as a user ID. Since Student ID was used as the e-mail address of the student, it was easy to leak outside. Student ID is constructed based on a department code and a serial number, so guessing other ID strings from one ID is easy. Student ID is issued at the day of the entrance ceremony, so it is not usable for pre-entrance education. Student ID will change when the student moves to another department or proceeds from undergraduate to graduate school, so he/she loses personal data when Student ID changes. To solve these problems, Kyushu University decided to introduce another unchanging user ID independent from Student ID. This paper reports the design of new user ID, ID management system we are using, and the effect of introduction of new user ID.

Categories and Subject Descriptors
K.6.5 [**Management of Computing and Information Systems**]: Security and Protection – *Authentication*

Keywords
Identity Management System; Service Continuity

1. INTRODUCTION
Universities provide various kinds of IT services such as e-mail, online course registration, e-learning and so on, to support students' learning, studying, and campus life. Usually a kind of "user identifier" is issued per user, and password authentication is used to identify and authenticate users for these services. For users' convenience, many organizations provide a unified identifier per user which can be used for various internal services instead of assigning different credentials per service [1][2].

Kyushu University also has various IT services for students. Most of them used user ID called "Student ID", derived from student number since 1995. Initially the authentication infrastructure using "Student ID" had been provided by the Educational Center for Information Processing as a part of IT education system (including Unix and Windows servers, PC terminals, e-learning system, etc to use during IT-related lecture courses). Now it is operated by the Information Infrastructure Initiative where we belong to. The use of Student ID has been expanded to other IT services operated by other departments such as course and record management system, syllabus system, library system, student portal etc.

Such ID has several advantages. Every student has one unique student number, so it is easy to uniquely identify a student by his/her Student ID. IT services operated by various departments don't need to maintain their own set of user IDs. The student number in Kyushu University includes a department code the student belongs to, and enrollment year. That information can be used for sorting/filtering a student list without additional metadata.

On the other hand, we gradually realized that using student number as user ID had some security risks. The student number isn't considered a secret, so it is weak against ID harvesting and brute force attack. For example, Student ID has been used as a local part (before the "@") of e-mail address due to historical reasons. Student number contains a serial number within a department, so it is easy to guess other possible ID strings from a Student ID and it can be used for reverse brute force attack (trying a trivial password against a large set of user IDs).

Also there were some difficulties providing services using student number. Student numbers are only finalized after finishing

admission procedures, and a student receives the number with his/her ID card at an orientation course just after the entrance ceremony. Some departments wanted to allow successful candidates of our university to use a part of IT education system and e-learning system for pre-entrance education, but it wasn't possible to use student number as a user ID. Another problem was the discontinuity of user accounts between undergraduate and graduate school students. Because a student number will change after proceeding to a graduate school, the same student was treated as a different user in various services such as e-mail, library, and storage services. These students had to migrate their data by themselves, and using the new Student ID as a graduate school student is not possible until receiving a new ID card.

To solve these problems, we decided to introduce a new user ID scheme specialized for intra-institutional IT services beginning in 2014. In this paper, we describe the design of new user ID scheme, its implementation and deployment, and the effect after the introduction of new user ID.

2. IDENTIFIER IN KYUSHU UNIVERSITY

First of all, we describe a brief history of user identifiers in Kyushu University.

2.1 Student ID based on Student Number

The Educational Center for Information Processing started to issue a unified user identifier for students since 1995. At that time, to provide education of the Internet and IT literacy, accounts for all the students were needed on their IT education system.

Student ID was introduced based on student number. A student number in Kyushu University consists of 9 characters shown in Figure 1. Due to the limitation of operating system at that time, user ID had to start from an alphabet and the maximum length allowed was 8 characters, so a student ID was generated by shuffling some parts of the corresponding student number, which caused confusion among new students.

Figure 1 Student ID until 2008

This conversion had been used until 2008, even after such a limitation had become obsolete in modern operating systems. Since 2009, student numbers has been used as-is for Student IDs.

2.2 ID for Staff Members

For staff members, the Information Infrastructure Initiative started to provide a unified user ID starting in 2007. We discussed the design of the ID scheme considering attack tolerance, usability, maintainability, and the number of users [3]. Finally we decided to assign a unique 10-digit pseudorandom number to each user as a user ID, and named "SSO-KID" (roughly meant Single Sign On - Kyushu University ID).

2.3 Identity Management System

As we mentioned in Section 2.1 and 2.2, Kyushu University had introduced an identity management system (IDM) for students first. The IDM for students was implemented as a part of the IT education system. After that, IDM for staff members was introduced separately by another company in 2007. We had to maintain and interconnect both IDMs, which complicated the entire system and repeatedly caused inconsistencies of user account data between them.

Upon replacement of the IT education system in the end of 2013 fiscal year, we decided to introduce a new, unified IDM containing data of both students and staff members, because IDM for students would also retire with the old education system. We considered it as an opportunity to introduce the new ID scheme for students similar to SSO-KID in order to solve problems with using "Student ID" derived from a student number.

3. REASONS FOR NEW ID SCHEME

In this section, we describe more details of issues using "Student ID" derived from a student number as a user ID and expected outcome by introducing new user ID scheme. The new scheme was similar to SSO-KID (for staff members), and called "Student SSO-KID".

3.1 Security Risk

We started to consider that security risks of using student numbers as user ID wasn't negligible. "Student ID" is (almost) the same as student number, and student numbers are not considered a secret. It is clearly printed on a student ID card, and commercial services offering discounts to students often make a copy of the face of the card or note the student number of a customer.

Historically, Kyushu University used "Student ID" as the local part of e-mail address of the student. For example, a student whose student number is "1AB14001X" is assigned an e-mail address "1AB14001X@s.kyushu-u.ac.jp". Recently we started to provide a service to create an alias of the e-mail address derived from the user's real name [4][5], but e-mail addresses based on student numbers are still actively used internally. As mentioned in Section 1, student numbers contains a sequence number, so it is easy to generate possibly valid IDs from one real ID obtained from outgoing e-mail messages.

If valid IDs are known, it is easier to intrude into an IT system by brute force attack. There were some incidents of e-mail account hijacking recently. We don't know the real cause of hijacking, but we decided to separate student number and user ID to mitigate some risks.

3.2 Service for Pre-entrance Candidates

In Kyushu University, a student number is issued when a candidate has finished the admission procedure after receiving an acceptance letter. The list of newly enrolled students is finalized at 17:00 on March 31st every year, so their student numbers can be finalized on April 1st or later. Actually the number will be available to these students on receipt of their student ID cards in the entrance orientation class after the entrance ceremony around April 7th.

As far as using Student ID, other university events which need to use IT systems have to be scheduled after giving student ID cards, but there were demands to offer services for pre-entrance candidates. For example, the information department wanted to provide an e-learning course to let them self-study about the basic knowledge of the university IT services. Also, the student affairs department wanted to allow early course registration for popular classes. To enable these services, we needed a new user ID scheme independent from student numbers.

To solve the problem, we decided to assign student SSO-KID to successful candidates and provide information about how to activate the account with an acceptance letter. The available space

of 10-digit SSO-KID is one billion, so assigning unique SSO-KID to candidates is not a problem. If a candidate declines, we just deactivate the SSO-KID and never use it again.

3.3 Health Checkup and PC Tutorial

In Kyushu University, all the undergraduate students must get a health checkup in the year of entrance and graduation. About 5,000 students get a checkup, so an efficient method is needed to identify who finished a checkup. Kyushu University requires all the students bring their own PC for learning [6], and a similar method is also needed in a Bring Your Own Device (BYOD) orientation class for newly enrolled students (around 2,700 participants).

Usually a student can be identified quickly by a barcode of the student number printed on his/her student ID card. But newly enrolled students need to get a health checkup and a BYOD orientation class before they receive their ID card, so we had to identify them manually. By providing the student's SSO-KID printed on an acceptance letter (with barcode), student identification should be far easier and efficient.

3.4 Continuity of User Accounts

As mentioned in Section 1, discontinuity of user accounts between undergraduate and graduate school students was also a problem. A student number changes after proceeding to a graduate school or moving to a different department. Due to that, the same student was treated as a different user in various services such as e-mail, library, and storage service. Such students had to migrate their data by themselves, or their data would be erased. The previous IDs are valid for one month after graduation for convenience, but that implies another security risk because students can use university's IT services for a while even after graduation.

By introducing student SSO-KID and assigning one unchanging unique ID to each student, students can use IT services without interruption and do not need to perform data migration. To do that, we need to track change of each student's student number appropriately.

4. DEPLOYMENT AND EFFECTS

In this section, we describe our strategy to introduce and deploy student SSO-KID, and effects observed after the deployment.

4.1 Deploy Strategy

As mentioned in Section 3, making a user ID independent from a student number should have many benefits. On the other hand, sudden change of the user ID scheme must be confusing from the users' perspective, and it is almost impossible to adopt the change to all the IT system in our university at once.

To allow easier and smoother transition of the user ID scheme, we decided on two deployment strategies. First, only new students enrolled in 2014 or later will use student SSO-KID as their primary user ID. Actually a student SSO-KID will be assigned to every student, but existing students will continue to use Student ID as their user ID until graduation or proceeding to graduate school. Second, to support IT systems which cannot adopt student SSO-KID by administrative or technical reasons, we will continue to provide a Lightweight Directory Access Protocol (LDAP) server which can authenticate users by Student ID.

4.2 LDAP Server Configuration

Kyushu University authentication infrastructure provides LDAP servers for intra-institutional IT services [7]. These LDAP servers provide user ID information in "*cn*" and "*uid*" attributes. Before introducing student SSO-KID, both *cn* and *uid* hold Student ID. To deploy student SSO-KID, we decided to provide two kind of LDAP servers as shown in (A) and (B) of Table 1. LDAP (A) is provided for services which cannot adopt student SSO-KID immediately. We encourage using LDAP (B) to gradually migrate from Student ID to student SSO-KID. We decided to keep Student ID in *cn*, because in some cases a system needs to search students by a Student ID or student number. Also by using a custom LDAP search filter, a system can authenticate students by both Student ID and student SSO-KID. We expect that LDAP (B) will become LDAP (C) within several years.

Table 1 User ID information in LDAP servers

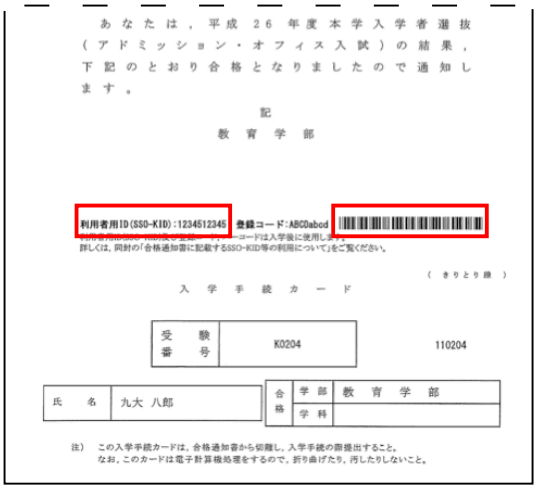
	(A)	(B)		(C)
	Legacy	Enrolled before 2014	Enrolled in 2014 or later	Student SSO-KID only
uid	Student ID	Student ID	Student SSO-KID	Student SSO-KID
cn	Student ID	Student ID	Student ID	Student ID

Upon introducing student SSO-KID, administrators of the e-mail system and campus cloud systems decided to use student SSO-KID for all the students. These systems implemented their own LDAP (C) server and populated the database by using data provided from the IDM system. Both systems happened to be replaced/upgraded at almost the same time as the IDM replacement, and it was decided to fully adopt student SSO-KID from the beginning.

4.3 Acceptance Letter

As mentioned in Section 3.2 and 3.3, student SSO-KID is included in an acceptance letter as shown in Figure 2.

The letter includes student SSO-KID, an activation code, and a


あなたは，平成26年度本学入学者選抜（アドミッション・オフィス入試）の結果，下記のとおり合格となりましたので通知します。

記

教育学部

利用者用ID (SSO-KID) : 1234512345 登録コード : ABCDabcd

詳しくは，同封の「合格通知書に記載するSSO-KID等の利用について」をご覧ください。

（きりとり線）

入学手続カード

受験番号	K0204	110204

氏名	九大 八郎	合格	学部	教育学部
			学科	

注） この入学手続カードは，合格通知書から切離し，入学手続の際提出すること。
なお，このカードは電子計算機処理をするので，折り曲げたり，汚したりしないこと。

Figure 2. An Example of Acceptance Letter

barcode of student SSO-KID. The activation code is required to activate the account using an online activation site, and after activation the student can use a part of IT education system and e-learning system in Kyushu University before entrance. The barcode is used to efficiently identify students in a health checkup and BYOD orientation.

4.4 Student ID Card

From 2014, student SSO-KID is printed on the back side of student ID card as shown in Figure 3. It was difficult to replace all the existing ID cards at once, and it was another reason we didn't deprecate Student ID immediately after introducing student SSO-KID. For compatibility with existing equipment, the barcode denotes student number, not student SSO-KID.

Figure 3 Backside of student ID Card (Old / New)

4.5 Effects

Until now, overall effects of introducing student SSO-KID have been favorable. For example, we reduced the reception process of a BYOD orientation class from 30 minutes to 5 minutes. Staff of health checkup also welcomed barcode of student SSO-KID printed on an acceptance letter because it simplified the process of new student identification greatly.

As mentioned in Section 3, introducing student SSO-KID has some benefits including lower security risks by reducing unnecessary exposure of user ID, providing pre-entrance services, and account continuity.

In 2014, pre-entrance learning materials were not fully prepared, but online learning classes were partially provided to some pre-entrance candidates, which was not possible before introducing student SSO-KID.

Because student SSO-KID was introduced in the end of 2013, almost all students still need to change their user ID from Student ID to SSO-KID when proceeding from undergraduate to graduate school, so the effect of account continuity wasn't notable. For the e-mail service, we designed the system that these students could change their user ID from Student ID to SSO-KID without service interruption. It was mostly successful in 2014, but partially broken in 2015 due to slight modification of the e-mail service and mismatching of account handling policy between IDM and the e-mail service. We had already sorted out the root cause of the problem, and are now discussing how to implement a solution.

5. CONCLUSION

In this paper, we described the design and deployment of a new student user ID for intra-institutional IT service in Kyushu University. Previously we used "Student ID" derived from student number as a user ID, but there were some security and usability concerns.

Beginning fiscal year 2014, we started to assign a student SSO-KID to every student which was a unique 10-digit pseudorandom value, and used it as a user ID for various IT services. By introducing student SSO-KID, several issues caused by using student number were solved. Especially the observed effect of a more efficient student verification process during new student's health checkup and BYOD orientation class.

We have to refine and improve account management and IDM operation continuously. For better support of account continuity, each IT system needs some modification, and legacy systems must be replaced. Many IT systems in Kyushu University are not under our direct control, and we need to encourage the use of student SSO-KID. Also, we will cooperate to implement better pre-entrance services for students.

6. ACKNOWLEDGMENTS

Our thanks to all the users using our IT services, and staff members of the authentication infrastructure working group to develop and maintain these systems in Information Infrastructure Initiative of Kyushu University.

7. REFERENCES

[1] Ito, E., Kasahara, Y., and Fujimura, N. 2013. Implementation and operation of the Kyushu university authentication system. In *Proceedings of the SIGUCCS 2013*(Chicago, IL, November 3 - 8, 2013). ACM, New York, NY, 137-142. DOI=http://dx.doi.org/10.1145/2504776.2504788.

[2] Ohta, Y., Kajita, S., Tajima, Y., Tajima, H., Hirano, Y., Naito, H., and Mase, K. 2010. Name Identification Method for Lifelong ID in Higher Educational Institutions. Journal of IPSJ, Vol. 51, No.3, 965-973. (In Japanese)

[3] Nogita, M., Kasahara, Y., Ito. E., and Suzuki, T. 2006. A Study of Identifier Naming Conventions Suitable for User Authentication. Technical report of IEICE. ISEC Vol.106, No. 411 (20061206), 67-72.

[4] Fujimura, N., Togawa, T., Kasahara, Y., and Ito, E. 2011. Primary Mail Service for students based on their names. *IPSJ SIG Technical Report*, Vol. 2011-IOT-14, No. 10, 1-6.

[5] Fujimura, N., Togawa, T., Kasahara, Y., and Ito, E. 2012. Introduction and experience with the Primary Mail Service based on their names for students. In *Proceedings of the SIGUCCS 2012* (Memphis, TN, October 17 - 19, 2012). ACM, New York, NY, 11-14. DOI= http://dx.doi.org/10.1145/2382456.2382460.

[6] Fujimura, N. 2013. Bring your own computers project in Kyushu University. In *Proceedings of the SIGUCCS 2013*(Chicago, IL, November 3 – 8, 2013). ACM, New York, NY, 43-50. DOI= http://dx.doi.org/10.1145/2504776.2504789

[7] Ito, E., Kasahara. Y., and Fujimura, N. 2012. A study of LDAP load balancing for University ICT services. *IPSJ SIG Technical Report*, Vol. 2012-CSEC-57/2012-IOT-17, No. 11, 51-56.