Case Study: Network System ID Conversion for a Connected Campus

Cecilia Iwala, Grambling State University

Abstract

Experience database users' access authentication procedure and learn the pros and cons of academic patrons' IDs conversion and the implementation process. This is a successful narrative and/or story of campus ID conversion and alternative ID creation in an academic institution. From this article, the reader can learn what to do and what not to do when converting campus user IDs, creating alternative users' IDs, or integrating new user IDs with existing IDs as security standards create the institutional need for alternative IDs for information accessibility and authentication. This article describes the process, the analysis, and the implementation of a campus network ID and management system. The 9-digit alphanumeric campus identification number (ID) is used in many places such as the student's ID card, registration information, admission and financial aid records, access to the university's banner web, and access to the library materials. The library authentication system uses a 9-digit numeric Personal Identification Number (PIN) for patron authentication purpose.

Keywords:

User authentication, user's ID, identity, identifier, database security, access control, remote access, and internet users (LAN & WAN).

Data definition and attribute abbreviations:

LAN/WAN: Local Area Network/Wide Area Network.

Authentication: In this review, authentication is the process of determining users' access to the computer network and electronic resources based on the patron's assigned username and password as related to application access control.

ID: Identification.

Gnnnnn: Example of the new campus ID. The alternative 9-digit alphanumeric characters issued to students, faculty, and staff members for user's information access and for security purposes.

ITC: Information Technology Center

PIN: Personal Identification Number.

ILS: Integrated Library System.

Key field: This is the first authentication field. The primary key and/or a crucial record identifier mostly used in relational databases.

Alternative field: This is the second authentication field. The alternative field provides a method to access data file other than the primary key.

Case Study: Network System ID Conversion for a Connected Campus

Introduction

Currently at the university level, Social Security number (SSN) as the student ID, is been replaced with a campus identification number known as the "campus ID. The ID is now being use as the primary identifier for all students, faculty, and staff members on campus and in accessing electronic resources. Without this campus ID in academic institution, student cannot access the university and the library resources. The population of students in our institution is 4,992 in which 4,538 were undergraduate students and 454 were graduate students. The total population of employees was 449. The institution was founded in 1901 with total degree programs of 67.

The new university patron ID was introduced in 2009 in order to help meet regulatory compliance that demands identity privacy protection for patrons. This is a network database user authentication to provide database access through external authentication network service. With this system, users' records are protected and access to the database systems must be verified by user's identity. In relation to user's privacy protection and access, according to Dasari [1], user's password is sent as a secret token to the server and the server authenticates user's identity. If a match is found for the password, the server grants access to the user to use the permitted services. As Systems Administrators, we facilitate password specifications for the system's users when we create a user. In the identity context, the user's ID is the digital representation of that individual's identity. Electronic or digital passwords are stored in the database and users can change their passwords at any time but most importantly, they need to remember the password and keep it secure.

This article describes the analysis, process, and implementation requirements in campus ID conversion process as a case study to help enhance the readers' understanding of network ID implementation processing. The article focuses on the system application requirements of the newly introduced campus ID implementation, how the problem was evaluated, the actions that were taken to provide accommodation for the new campus ID, and the successful implementation of the ID conversion.

The ID discussed in the article is related to user authentication with security systems as the process of identifying an individual or a person based on the database access assigned identity, and to also make certain that the individual is who he/she claims to be through the username and password. A user's knowledge of the password is assumed and/or understood to guarantee that the user is authentic. According to Dobromir Todorov [2], user identification and authentication are essential parts of any information security system. Todorov [3] believes in information security as applied to computers and networks. Consequently, he emphasizes that users should authenticate as they access their computer systems at work or even at home every day.

Data conversion

To successfully convert users' IDs, integrating or creating alternative IDs for any system, the Systems Administrators and/or Librarians need to have comprehensive knowledge of the current data structure of the patrons' records and need to understand the following information: the current data structure of the patrons' records, what ID field to use as the key ID field or primary key, and what to use as the alternative ID field in the authentication record in relation to the organization of the patrons' files.

Converting and integrating new IDs to existing IDs requires thorough steps and techniques. When we started the conversion at the library, we communicated the project's goals and objectives to the campus Information Technology Center (ITC) staff and discussed the structure and formation of the existing patron IDs with ITC staff and other library staff as well as external stakeholders, such as vendors. We requested the existing patron files and verified the format, structure, and authentication field of the patron files. We conveyed the information to the LOUIS group (Louisiana Online University Information System) and performed more analysis on the patrons' files formation for effective conversion. Credit is given to the LOUIS staff, especially to Mary Laird for assistance rendered during the ID conversion and implementation period. She provides the necessary integrated data compatibility information needed by ITC staff for the formation and/or configuration of the ID file.

After analysis of the data, we discovered that the system has only one field as a key field in the ID record with a blank alternative field. In order to accommodate the new campus IDs and determine the relationship between the two ID fields, which is to link the new IDs with the existing IDs successfully, we had to first define and make a provision for the alternative field in the patron file table to help accommodate the new campus IDs. Subsequently, we had to determine a method to establish a relationship between the patron alternative ID and the Key or primary ID for effective authentication and conversion process. The alternative ID field is needed for users' authentication due to security standards required by the institution.

Challenges

Threats include issues of integration of the new campus IDs into the existing system/program. The existing integrated library system (ILS) equipment, such as the student ID card readers or scanners, was designed to capture library patron data with numbers only and not alphanumeric data. The new campus ID includes alphanumeric data, so additional conversion and/or modification was necessary to accommodate this data type for effective authentication and integration of the information.

Resolution

The campus ITC department assisted in converting the letter (G) in the beginning of every patron record into a digit and/or number (9), enabling library equipment, like the ID card readers, to successfully read the data from the patron cards and extracts the information into the system applications.

Patron files load principles

Before the implementation of the system, the patron file was using the patron's Social Security Number (SSN) as its only ID field. As a Systems Administrator/Librarian, I worked collaboratively with ITC technical support staff to accommodate the new patron ID. We generated two types of patron files based on the specifications provided by the consortium. The first patron file consisted of two authentication ID fields with SSN on both fields (the key field and the alternative field). The second patron file consisted of two authentication ID fields with the new campus ID on the key field while the SSN was on the alternative field.

In the first patron file load, the SSN was on both fields as indicated above and the system loads the file using the key IDs to create and update patron records. This established the foundation and created the required fields for the new records. The patron's SSN was used to find matching records since it is unique and no two patrons can have the same Social Security number. Ideologically, we believe that everybody has a Social Security number but not everyone has the campus ID yet since the campus ID is new to every user.

In the second patron file load, the campus ID was in the key field and the SSN was in the alternative field. The system uses the SSN in the alternative field as the match point for user ID creation.

The system matches patron records with the SSN to load the database table and replaced the key field of the existing table (the new campus ID replaces the SSN that was previously created with the first file load). This completely established the access authentication foundation for the new campus ID while still maintaining the alternative field (SSN). At this point, it makes sense to use the campus ID as the key field since the institution is heading towards using the campus ID for authentication instead of the patron's SSN for protecting patron privacy.

Application logical function during patron file load, the system looks for the ID key field (Gnnnnn) and when a match is found, it updates the record. Alternatively, for any record for which a match is not found in the key field, the system looks for the alternative ID field (SSN to find a match and then updates that record. If no match is found on both the key and the alternative fields, the system will therefore create a new

record for the patron with the campus ID in the key field and the SSN as the alternative field.

When we completely established and accommodated both the key and the alternative IDs in the system database table, we then proceeded to simply use the key field for update and for creating new patron's record. In other words, future patron file loads now use the new campus ID as the key field. Please see Figure-1 of the Network ID System Authentication Process for a detailed illustration.

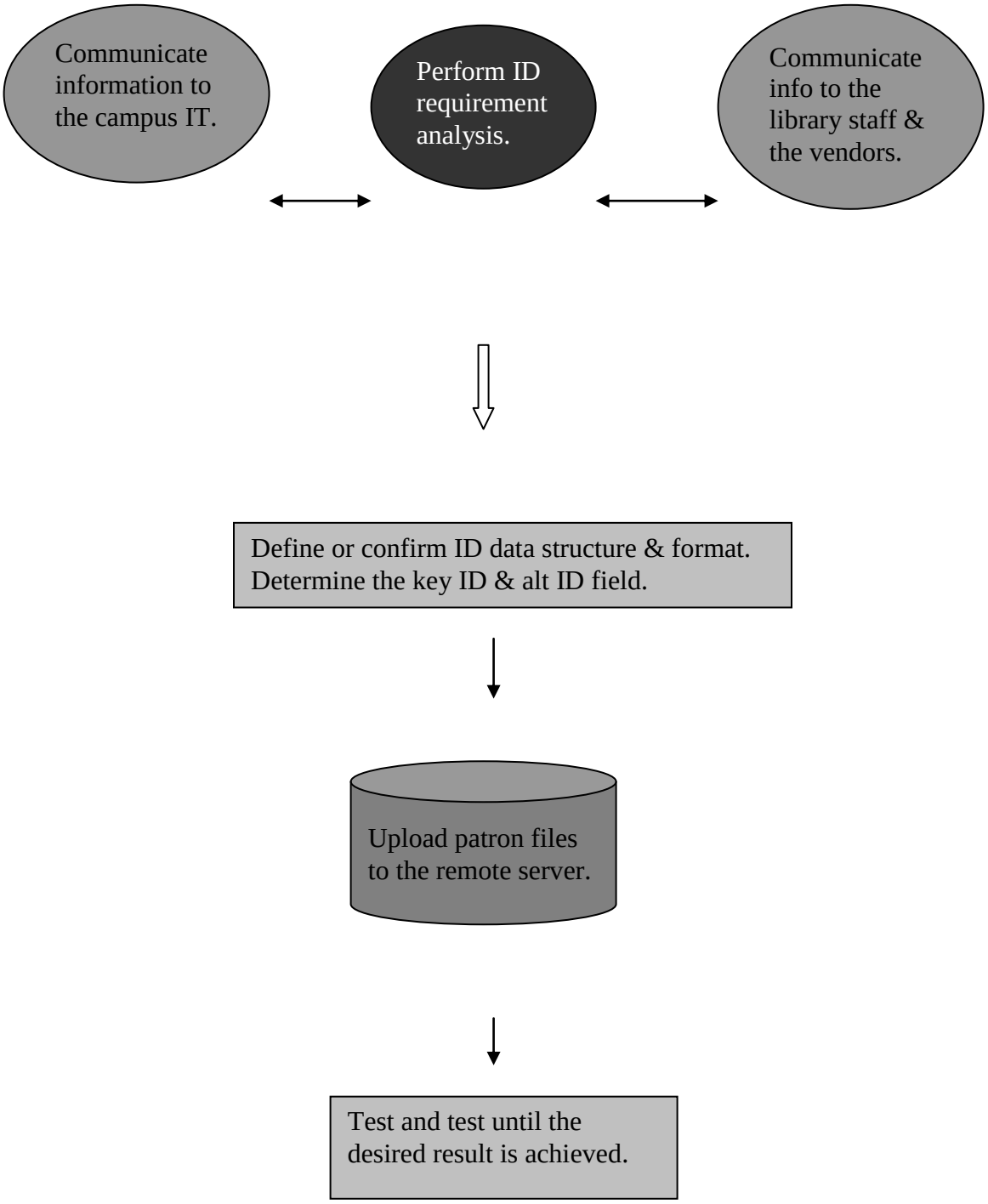
Manually

Patron status can be verified and a new patron/user can be added manually to the authentication system by authorized library staff. When verifying a user's access, if the following message "patron not found" appears, it means that there is no match for the user in the database. Staff can search for the patron either by using the campus ID or the patron's SSN depending on the ID card the patron is using since many users are still carrying an old ID cards without campus IDs. If a patron record already exists, the library staff will carefully verify the patron's name and proceed with the patron's request. In this case, the patron is in the system but with one authentication ID instead of both IDs. If the staff member has editing authority, he/she can manually modify the patron record to add the missing information. Otherwise, the patron will wait until the next patron file is loaded to correct the single ID error. If no patron record exists with either ID for the user, and the staff member has the authority to create and provide access to the user, he/she can then register the patron.

In summary, to successfully implement a system ID in an academic library, the Systems Librarians need to analyze the system requirements, understand the current patron application, understand the data structure of the existing and the new patron files, and establish a plan to accommodate the ID and maintain the system. The Systems Administrator needs to determine the relationship between the key field and the alternative field for the ID if using two ID fields and, as necessary, create logic schemas and/or the dataflow of the ID system. The Systems Librarians/Administrators need to establish specifications for data format and configuration. Most importantly, the Systems Librarian and/or Systems Administrator needs to perform system testing and data validation to detect errors, since validation confirms that the implemented system conforms to the original requirements established for it. Finally, the Systems Librarian needs to communicate and present the findings to the stakeholders and create or set up implementation plan for the system.

During system testing, we first downloaded the patron files into the SirsiDynix Symphony remote server in the training module. We then specified the file loading logic and procedures by using the student's alternative ID (the SSN) and instructing the system to also update the student's new campus ID. We instructed the system to create and update students' records in the test only environment and to also perform dynamic indexing (automatic instant indexing). This helped us to see how the information is going to be loaded and recorded in the training system before proceeding to the production environment. See the Network ID System Authentication Process Overview schema in Figure-1 for more information.

Figure-1 Network ID System Authentication Process Overview.



Created by Cecilia Iwala-Olufarati.

Users can secure access to the database information from inside the university and also from outside through the network firewall (LAN/WAN).

Conclusion

In conclusion, this study builds on the understanding of the role of Systems Administrators and Librarians values in the implementation of user IDs, especially in academic institutions. This study directly addresses many of the core issues facing Systems Administrators and Librarians including steps and procedures in users' IDs creation, conversion, and day-to-day user account management. This case study provides suggestions and recommendations for effective patron ID implementation, including issues and challenges of digital ID creation and password storage and management techniques in the library context.

The audience that benefits from this study includes Systems Administrators and Analysts, Systems Librarians, Developers or programmers, Information Security Analysts, Information Technology Managers, Systems Technicians, systems users, students and faculty members, university and library staff and/or anybody that cuddles or have interest in the library and technology context.

Spangler Todd, "VPN Services Check Digital IDs." *Inter@ctive Week* 6, no. 8 (1999): 28.

[1] Nagamalleswara Rao Dasari and Vuda Sreenivasarao, "Performance of Multi Server Authentication and Key Agreement with User Protection in Network Security." *International Journal on Computer Science & Engineering* 2, no. 5 (2010): 1705-1712.

[2] Dobromir Todorov, *Mechanics of User Identification and Authentication: Fundamentals of Identity Management* (Boca Raton: Auerbach Publications, 2007).

[3] Ibid.