Cooperation between the Temporary ID Card Registration System and Access Control System

Author: Koki Okunishi*

The employee identification (ID) cards distributed at all Mitsubishi Electric business bases in Japan use a contactless-type IC card with a uniform format, which can be registered to the access control system at Mitsubishi Electric headquarters. We built a cooperative system that temporarily registers these ID cards to the access control system at headquarters for improved convenience and security.

1. Background

Since 2005, for the purpose of corporate governance, Mitsubishi Electric has introduced access control systems using contactless IC cards at Mitsubishi Electric’s branch offices, sales offices, manufacturing bases, factories, laboratories, and other business bases in Japan. Meanwhile, in November 2005, Mitsubishi Electric moved its headquarters to the Tokyo Building, where the Mitsubishi Electric MELSAFETY system was introduced to perform access control using employee identification cards.

The Mitsubishi Electric employee ID cards are contactless IC cards with a uniform format, and are distributed at the company headquarters as well as at all business bases in Japan. Therefore, we are technically able to register all employee ID cards to the headquarters access control system. However, in order to avoid safety and administrative risks, this is not permitted, and instead temporary guest cards are issued to internal visitors from other business bases within the company.

Each internal visitor presents his/her ID card and then receives a temporary guest card, resulting in a waiting line at the reception desk at headquarters. In addition, internal visitors waiting to receive a guest card may keep external guest visitors waiting.

Consequently, for improved convenience and security, we built a system for internal visitors, which temporarily registers a Mitsubishi Electric employee ID card to the headquarters access control system.

This paper describes the configuration of this system.

2. System Requirements and System Configuration

The requirements for the temporary ID card registration system to be introduced at Mitsubishi Electric headquarters are as follows:

1. To be able to use the existing MELSAFETY access control system;
2. To be able to use the existing employee ID cards;
3. To be able to use the existing employee identification information server;
4. To cooperate with the newly introduced visitor acceptance application server;
5. ID card registration to the existing MELSAFETY security system is to be valid for use by the visitor only during the period of his/her business trip; and
6. Security gates and card readers available for each internal visitor are to be restricted to those within his/her accessible area.

To satisfy the above requirements, we coordinated the existing systems to develop the temporary ID card registration system that realizes the required functions. Figure 1 shows a diagram of the entire system configuration.

The temporary ID card registration system receives the application of an internal visitor from the visitor acceptance application server, extracts the visitor’s ID card information from the employee identification information server, and registers the information to MELSAFETY. For efficient system development, we used "DIGUARD NET", Mitsubishi Electric’s own security system integration platform to interface with MELSAFETY.

3. Basic System Functions

The process flow of the temporary ID card registration system is as follows:

1. An application entry for the visit is sent from the visitor acceptance application server;
2. The interfacing function of the visitor acceptance application server receives the application data and registers it to the task management function;
3. The task management function checks the schedule of application entries, and then notifies the user information delivery function of those that have ex-
pired and those that are valid;

(4) Based on the application data notified from the task management function, the user information delivery function retrieves the user information from the employee identification information server, and

(5) The user information update function reflects the received user information and visiting period on MELSAFETY.

In preparation for the occurrence of a mismatch between the task management database and MELSAFETY, this system also has an all-tasks delivery function to correct the mismatch by notifying the information of all tasks to be delivered at that moment.

To realize the above process steps, we developed the basic system functions shown in Table 1. Figure 2 shows the internal module configuration of the temporary ID card registration system.

4. System Construction (Ensuring Compliance with the Company Security Policy)

In accordance with Mitsubishi Electric’s security policy, no direct connection is allowed between a physical security system and an information system, and if any connection is made it must be via a firewall.

<table>
<thead>
<tr>
<th>No.</th>
<th>Function</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Visitor acceptance application server interface</td>
<td>Receives the application data and provides it to the task management function</td>
</tr>
<tr>
<td>2</td>
<td>All-tasks delivery command</td>
<td>Executes delivery of all tasks</td>
</tr>
<tr>
<td>3</td>
<td>All-tasks delivery interface</td>
<td>Calls for the all-tasks delivery function</td>
</tr>
<tr>
<td>4</td>
<td>Task management</td>
<td>Controls and provides the task information to the user information delivery function as needed</td>
</tr>
<tr>
<td>4-1</td>
<td>Task registration</td>
<td>Registers the entered task information to the task DB</td>
</tr>
<tr>
<td>4-2</td>
<td>Regular task delivery</td>
<td>At each predetermined time, checks the information in the task DB and delivers the required information to the delivery management function</td>
</tr>
<tr>
<td>4-3</td>
<td>All-tasks delivery</td>
<td>Provides the information contained in the task DB to the delivery management function</td>
</tr>
<tr>
<td>5</td>
<td>User information delivery</td>
<td>Delivers the provided task information to MELSAFETY</td>
</tr>
<tr>
<td>5-1</td>
<td>Delivery management</td>
<td>Sends the provided information to the MELSAFETY delivery function and DB delivery function</td>
</tr>
<tr>
<td>5-2</td>
<td>MELSAFETY delivery</td>
<td>Delivery to MELSAFETY</td>
</tr>
<tr>
<td>5-3</td>
<td>DB delivery</td>
<td>Registers to/deletes from the DB</td>
</tr>
<tr>
<td>6</td>
<td>User information update</td>
<td>Reflects the user information on MELSAFETY</td>
</tr>
<tr>
<td>7</td>
<td>User information acquisition</td>
<td>Retrieves the user information and ID card information for a specified user from the employee identification information server</td>
</tr>
</tbody>
</table>
The MELSAFETY access control system is categorized as a physical security system, whereas the visitor acceptance application server and the temporary ID card registration system are categorized as information systems; thus, direct connection between these systems is not permitted. Consequently, we have chosen to set up a relay server to relay the user information delivered from the temporary ID card registration system to MELSAFETY.

To pass through the firewall, we adopted HTTP as the protocol between the temporary ID card registration system and the relay server; for the communication between the relay server and MELSAFETY, we adopted DIGUARD NET. Therefore, we designed the relay server to convert the information to be registered. The relay server operates as follows:

1. The user information to be registered is received from the temporary ID card registration system via HTTP;
2. The user information to be registered is output to a link file, which is then written to the shared folder of the MELSAFETY access control system;
3. The file that contains the registration results from the MELSAFETY access control system is read and the registration results are sent back to the temporary ID card registration system via HTTP; and
4. The temporary ID card registration system receives the registration results; if the user information was not registered, the system repeats the registration of the user information.

Since we designed this system using a relay server and DIGUARD NET, construction of the system was easy even in an environment such as headquarters where no direct connection is allowed between a physical security system and an information system. This technology can easily be deployed at other business bases as well.

5. Operation after System Installation

The operation steps of this cooperative system are explained using Fig. 3:

1. The internal visitor emails or phones the host person to provide his/her name and the date of the business trip, and requests an application for entry using his/her ID card;
2. The host person uses the workflow on the website to enter the name of the visitor (if more than one visitor, the names of all visitors) and the date of the business trip, and to ask his/her manager for authorization;
3. The manager reviews the application on the workflow, and gives the authorization;
4. The authorization is notified to the visitor by email;
5. The visitor confirms the registration by email, and visits the headquarters with his/her ID card;
6. The visitor presents his/her ID card at the security...
gate located at the side of the headquarters reception, and then enters the offices (no check-in process is required at the reception desk); and
(7) The visitor also presents his/her ID card to the reader when he/she enters any room in the headquarters offices.

Since the workflow entry screen in the above Step (2) is provided as a web page, the host person can enter the data from the PC on his/her desk. An example of the entry screen is shown in Fig. 4.

As described above, the introduction of this system allows an internal visitor, by communicating in advance, to enter any place within the headquarters using his/her own ID card, and eliminates the check-in process or the use of the guest card, resulting in improved convenience.

In addition, the guest cards that used to be manually handed out at the reception desk are now automatically distributed. The automated process eliminates mistakes in recognizing individuals, wrong distribution, or false recording, for improved security and traceability.

6. Effect of Introduced System
In February 2009, we started test operation of this system. About a month later, we conducted a questionnaire survey for the users. As a result, 97% of the users felt that “convenience was improved”, indicating the huge effect of the system’s introduction.

In addition, since introducing the system, Mitsubishi Electric employees no longer need to wait in a line at reception to receive their guest cards. As a result, external guest visitors have a shorter wait for their guest card. Figure 5 shows a photograph of the reception desk at Mitsubishi Electric headquarters after the introduction of this system.

7. Future Prospects
Our newly developed temporary ID card registration system, which was introduced at Mitsubishi Electric headquarters, makes it possible to temporarily register an employee ID card. We intend to introduce this system at all Mitsubishi Electric business bases in Japan, aiming at the improvement of both convenience and security throughout the company.

We also plan to improve the system not only for in-company use but to promote it as an optional product of the MELSAFETY access control system.