

# Identity Lifecycle Management Technology

Authors: Seiichi Kondo\* and Tatsuya Tsurukawa\*

## 1. Introduction

In an integrated identity management system for shared use by the types of security components of a corporate information system and business operation system, the lifecycle should be managed in accordance with the organizational structure of the corporation in order to reduce operating costs associated with types of variations, to maintain and improve the security level, and to ensure digital traceability.

## 2. Identity Management and Problems

An identity management system manages information concerning identity and access privileges assigned to users. As shown in Fig. 1, the identity information is uniformly managed by the database for safe and efficient user authentication and authorization. The identity information is distributed to the controlled access management system and business applications, etc. The identity information is also used for authorization concerning user authentication and access privileges employed in various systems such as PC log-on, removable devices control, file encryption, and single sign-on for Web based applications.

Lifecycle management of the identity management system is required to deal with the following variations which may arise after the system has been introduced due to the company's activities.

(1) Variations in information of identity and access policy

User attribute information which is the basis of access control changes in accordance with employment, retirement, transfer, promotion, and re-organization. And also security targets such as devices, contents are added or removed, and policy improvement is done in accordance with internal or external factors.

(2) Variations in authentication device that identifies users

Smart cards identifying employees and visitors are increasingly being used for various types of applications. However, these cards are at risk of loss, contamination, damage, failure, and theft. To ensure operational safety, a quick response and appropriate measures in accordance with the security policies are necessary.

(3) Changes in user information of identity in log stored for a long time

Security Standard ISO/IEC 27001:2005 specifies regarding the acquisition of audit logs that an audit log containing the records of user activities, exception handling, and information security events shall be recorded and the log shall be stored for an agreed period in case of future investigations and for monitoring access control. Generally, such logs are held for a long time, and precise association with information concerning identity, devices, and contents which often change during the storage period becomes an important issue.

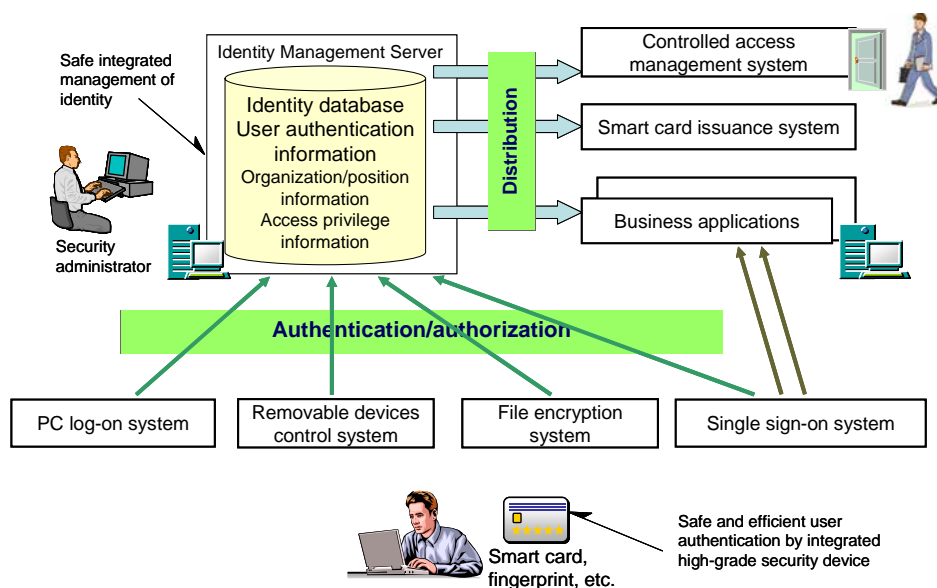


Fig. 1 Architecture of identity management system

This report introduces solutions to such problems in the following sections 3 to 5.

### 3. Identity Management for Corporations

The RBAC (Role-Based Access Control) model<sup>(1)</sup> is widely used for access control with security objects such as devices and contents separated from users. In RBAC, changes in user information and security objects are localized by connecting the users and permission for operating security objects indirectly via a role. A hierarchical RBAC employs a hierarchical role. As discussed in Section 2 (a) above, corporations generally define roles on the basis of personnel information such as their organizations and positions, so there is an issue that changes in personnel details significantly affect the settings between roles and users.

To solve this problem, we propose the structure shown in Fig. 2 (b), in which the users and the organization associated with the personnel information are assigned independently from the roles. The relationships between roles and the organization and between roles and users are indirectly designated by rules defined by logical formula instead of directly connecting them. As a result, the influence of changes in personnel

information on roles can be localized.

### 4. Smart Card Implementation Management

Corporations today increasingly use smart cards as employee IDs for controlling access to corporate facilities, logging on to PCs, approval, print-out authorization, etc. As discussed in Section 2 (2), it is necessary to change the access privileges, change to substitute cards, and output audit logs quickly and accurately whenever the details of smart card users change due to personnel relocations or business trips, and whenever smart cards are affected by loss, contamination, damage, failure, theft, or expiration of validity as shown in Fig. 3. Especially when smart cards are changed to substitute cards, how to maintain conformance between the official cards and substitute cards with respect to the combinations of conditions of cards is the key issue.

We propose the system shown in Fig. 4 in which smart card implementation rules are defined in a state chart to construct the implementation system without needing a program. The implementation rules are defined and operated as follows.

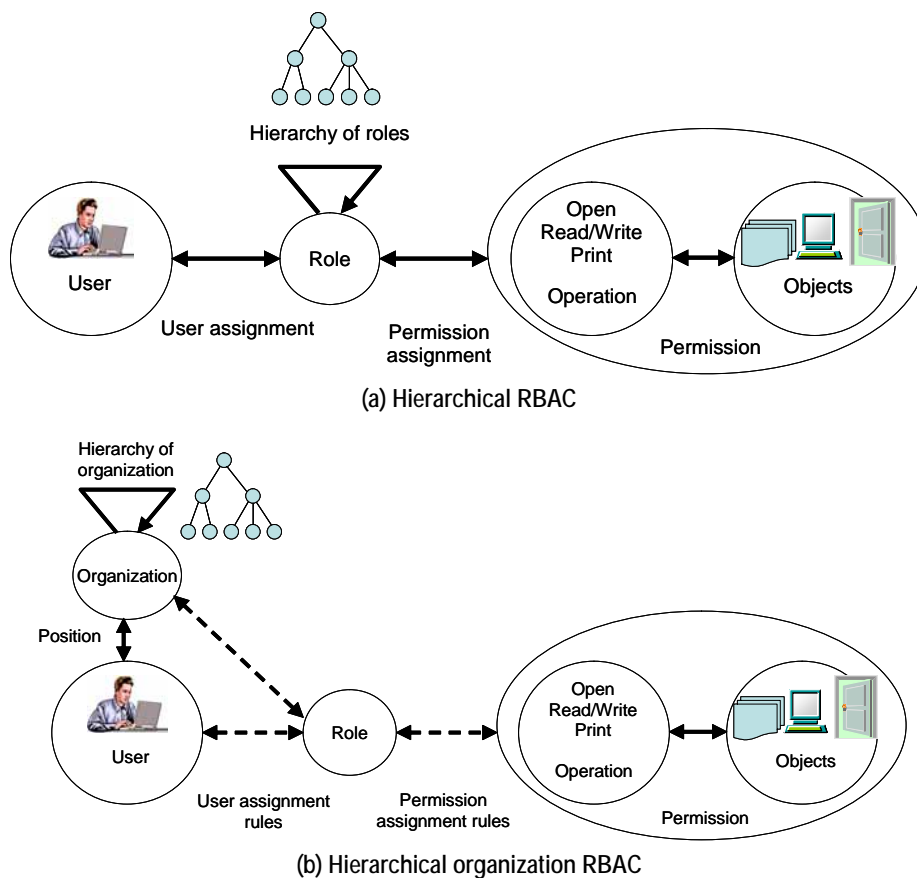


Fig. 2 Role-based access control (RBAC)

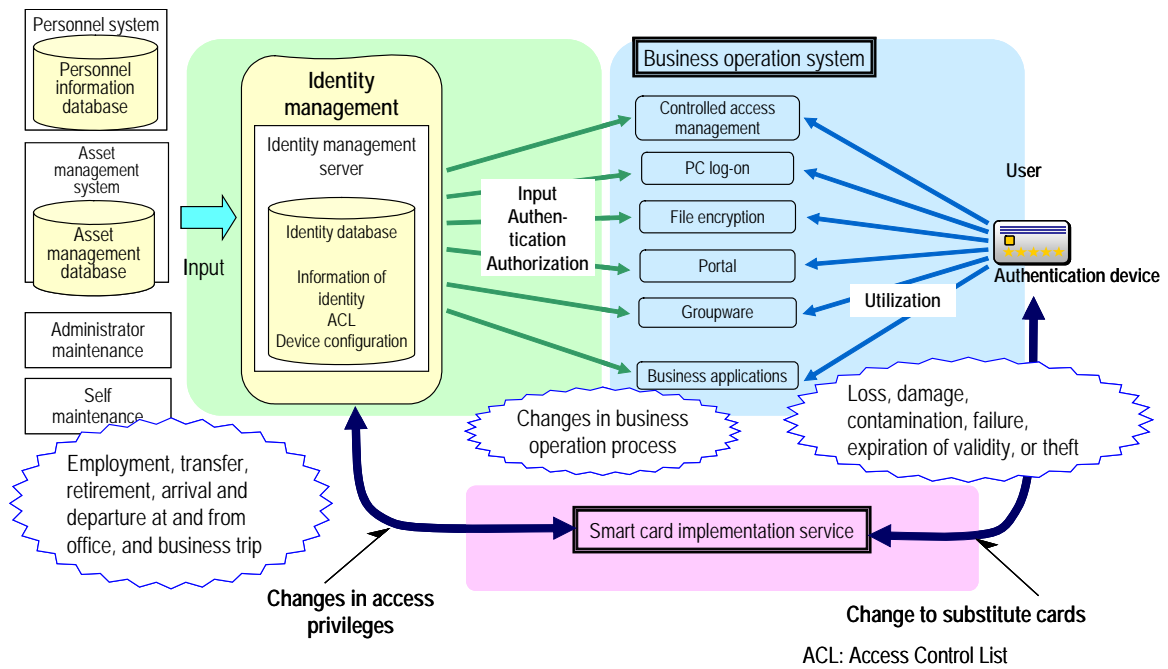


Fig. 3 Example of smart card management system

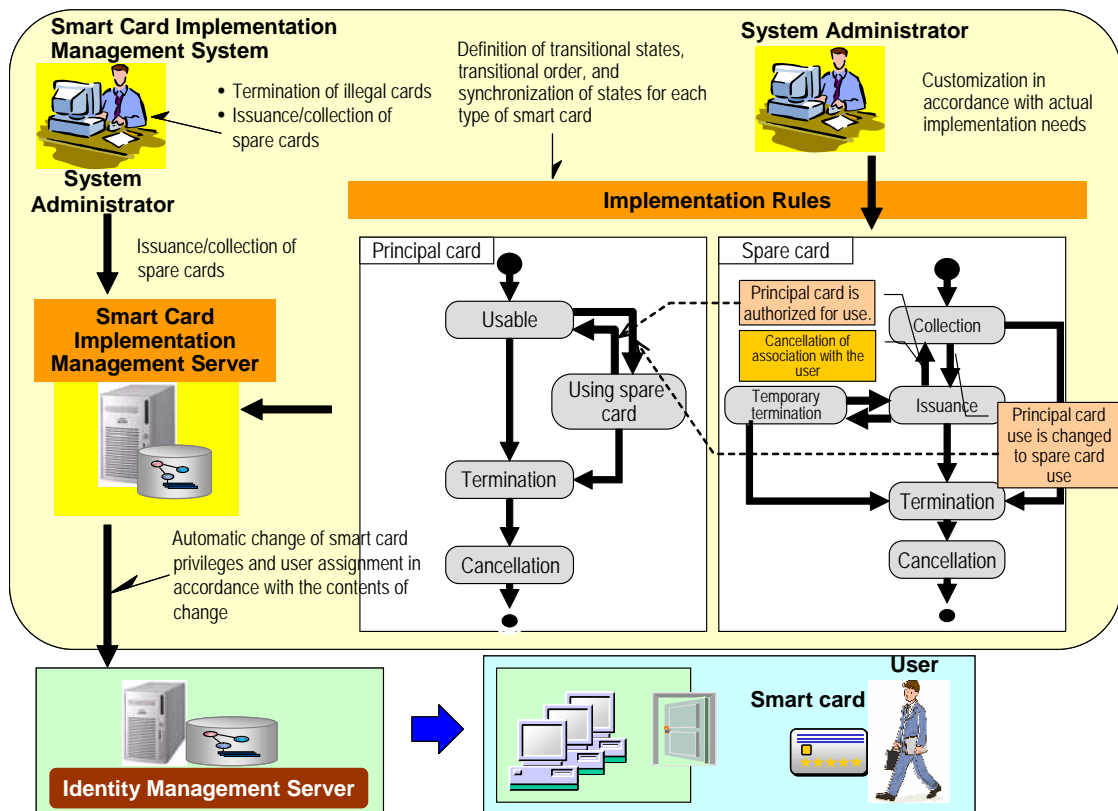


Fig. 4 System example using implementation rules

- (1) The changes in the conditions of cards for employees, cards for nonemployees/residents, cards for visitors, and spare cards in case of accident are defined dynamically and independently from the program in the state chart as shown in Fig. 4.
- (2) The changes in access privileges due to changes in the conditions or the restriction that the cards cannot be used simultaneously with the corresponding spare cards are defined as actions.
- (3) The actions in accordance with the changes in the conditions are automatically executed according to the implementation rules defined in items (1) and

(2) above.

This configuration of implementation rules, which is independent of the program, has the following effects.

- Improved security level  
Conformance of conditions among two or more cards and automation of the function interlocked with the access privilege control prevent users from improper use, whether deliberate or accidental.
- Application of implementation rules to different environments  
Required implementation rules of smart cards can be used for different divisions without a program.

### 5. Digital Traceability

This section examines digital traceability which governs logs stored for a long time under a change of user information, as mentioned in Section 2 (3). Today, various systems collect and store the logs output by various application programs as well as the systems themselves, so that the causes of any information leaks could be analyzed. However, disagreement of user identifiers recorded in the logs for respective sources often prevents multiple logs from being analyzed in an integrated manner. To resolve this, digital traceability can improve log analysis by combining the identity management system which provides the identity lifecycle management function in response to changes in employment, transfer, and retirement of employees over a long time, as one of its characteristic functions.

Focusing on the user identifiers recorded in the

logs, the problems in using them are listed below.

- Difficult to uniformly analyze multiple logs  
Because the user identifiers are recorded with identifiers unique to each log, it is difficult to execute a uniform analysis spanning different logs.
- Attribute information of users cannot be used for analysis.

The attribute information (e.g., names and divisions) associated with the respective user identifiers is usually not recorded, and so cannot be used for analysis.

Figure 5 shows an example of a system configuration using digital traceability. The logs are collected from terminals, servers, and physical security equipments and stored in the log management server. The system also has an identity management server providing identity management function, and a management terminal that retrieves and displays the logs from the log management server.

- Inquiry and reflection of unified identifiers

The log management server, after collecting logs, makes inquiries with the identity management server to obtain the unified identifiers associated with the log-specific user identifiers stored in each log and reflects them in the logs for storage.

Logon account or E-mail address are examples of the log-specific user identifier above and the unified identifier above means the identifier which can uniquely identify the particular user like an employee No.

Inquiring and reflecting unified identifiers to all log records enables links between user identifiers recorded

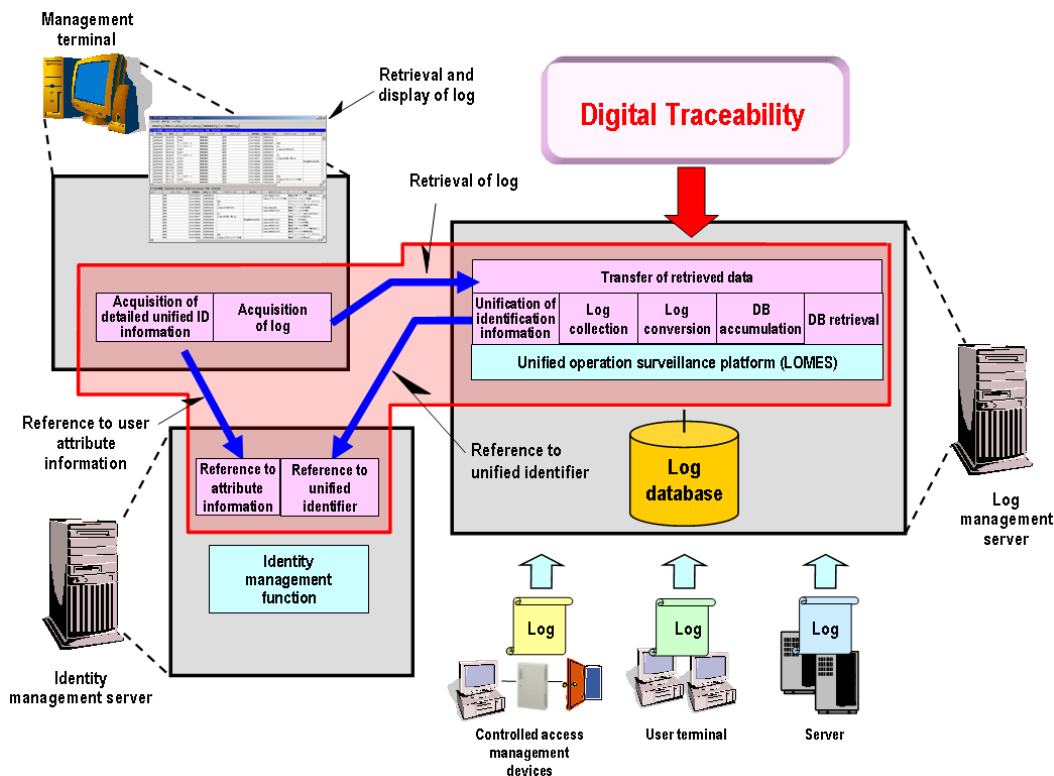


Fig. 5 Example of system configuration with digital traceability system

differently in each log and then makes uniform log analysis available.

- Analysis using attribute information

After retrieving and displaying a log on the management terminal, it can inquire a part of the attribute information associated with the unified identifier and it also can display them additionally (see Fig. 6). If all the attribute information is reflected in the accumulated log, the log becomes large and inefficiently consumes the capacity for the log database. However, it reflects them after retrieving and narrowing down the log, thus solving the problem and allowing the system to use the attribute information efficiently during log analysis.

Likewise, in combination with the identity management server, log analysis with referencing corresponding personnel affair information can be available by inquiring and displaying them as necessary (see Fig. 7). Even if

the log to be analyzed is old and the corresponding user has retired, past logs still can be analyzed with the relevant personnel information based on the date and time of the log record.

We have stated the integrated management of identity and the lifecycle management for diversified changes of it, they are necessary to enable the governance of information systems.

We are going to seek "comfort" enabling convenience, "safety" by system automation, and "development" by providing identity history to logs in the identity implementation management.

**Reference**

R. S. Sandhu, D., et al.: Role-Based Access Control Models, IEEE Computer, 29(2): 38-47 (1996)

User ID	...	Output File	Operation
0010022		CustomerList2005.pdf	Audit (File update)
0020013		CustomerList2005.pdf	Audit (File export)
0010007		CustomerList2005.pdf	Audit (File print)
0010017	Cu		
0020011	Cu		
0010018	Cu		
0010028	Cu		

User ID	Name	Division	...	Output File
0010022	Smith	Personnel		CustomerList2005.pdf
0020013	Green	Accounting		CustomerList2005.pdf
0010007	Barnard	Engineering		CustomerList2005.pdf
0010017	Radford	Sales		CustomerList2005.pdf
0020011	Moore	Personnel		CustomerList2005.pdf
0010018	Kim	Sale		CustomerList2005.pdf
0010028	Johnson	Engineering		CustomerList2005.pdf
0010014	White	Accounting		CustomerList2005.pdf

Fig. 6 Integrated indication of attribute information

	Past	Present
Date Time	2005/03/09 12:48:34	2006/03/09 13:35:54
Unified User ID	0010026	0010026
Name	Taro Mitsubishi	Taro Mitsubishi
Division	Accounting	Personnel
Title	Assistant Manager	Manager
Employee Type	Regular Staff	Regular Staff
Qualification		
Employee No.	0010010	0010010
E-mail address	taro@domain.co.jp	Mitsubishi.Taro@domain.co.jp
TEL	03-1234-5678	03-1234-5678
Extension	9876	5432

Fig. 7 Indication of past and present personnel information