Z Specification Example

Computer System Version 1

1 Introduction

A computer system that has multiple domains: Admin, Purchase, Retail and Booking. It also has multiple departments: Estates, Sales, Management, Office. The following table defines which Department members can login to which Domain.

	Admin	Purchase	Retail	Booking
Estates	x	x		
Sales		x	x	x
Management	x	x	x	x
Office	x	x		

2 Types

[STAFF] set of all uniquely identifiable employees

3 The State of the System

Computer

$users, loggedIn : \mathbb{P}\, EMPLOYEES$

$loggedIn \subseteq users$

4 Initialisation

InitComputer

$Computer'$

$loggedIn' = \emptyset$
$users' = \emptyset$

5 Change State Operations

Partial Operations defined here are:
i) Add User
ii) Remove User
iii) Log in
iv) Log out

5.1 Add User

Adds a new user. It specifies that p? is a member of staff and should not be a member of users before the operation. It also specifies users' will include the new user, p? Any implementation should also not allow a change to the loggedIn set after the operation.

$$
\begin{array}{|l}
\hline
\textit{AddUser} \\
\Delta Computer \\
p? : STAFF \\
\hline
p? \notin users \\
users' = users \cup \{p?\} \\
loggedIn' = loggedIn \\
\hline
\end{array}
$$

5.2 Remove User

Removes a user. It specifies that p? is a member of staff and constrains p? to be a member of users before the operation. It also specifies that p? will be removed from users'. Any implementation should also ensure that p? is not logged in before the operation. Any implementation should also not allow a change to the loggedIn set after the operation.

$$
\begin{array}{|l}
\hline
\textit{RemoveUser} \\
\Delta Computer \\
p? : STAFF \\
\hline
p? \in users \\
users' = users \setminus \{p?\} \\
p? \notin loggedIn \\
loggedIn' = loggedIn \\
\hline
\end{array}
$$

5.3 Log In

The basic log in specification is logIn. It specifies that p? is a member of staff and should be a member of users before the operation. It also specifies that p? should not be a member of loggedIn before the operation. It also specifies loggedIn' will include the new user, p? after the operation

$$
\begin{array}{|l}
\hline
\textit{LogIn} \\
\Delta Computer \\
p? : STAFF \\
\hline
p? \in users \\
p? \notin loggedIn \\
users' = users \\
loggedIn' = loggedIn \cup \{p?\} \\
\hline
\end{array}
$$

5.4 Log Out

The basic log out specification is logOut. It specifies that p? is a member of staff and should be a member of users before the operation. It also specifies that p? should be a member of loggedIn before the operation. It also specifies that p? will be removed from loggedIn' after the operation and that there will be no change in the set users' after the operation.

$$
\begin{array}{|l}
\hline
\textit{LogOut} \\
\Delta Computer \\
p? : STAFF \\
\hline
p? \in users \\
p? \in loggedIn \\
users' = users \\
loggedIn' = loggedIn \setminus \{p?\} \\
\hline
\end{array}
$$