

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

[EMPLOYEE] set of all uniquely identifiable employees

3 The State of the System

<i>Computer</i>	_____
<i>users, loggedIn</i> : $\mathbb{P} \text{ EMPLOYEE}$	
<i>loggedIn</i> $\subseteq$ <i>users</i>	

4 Initialisation

<i>InitComputer</i>	_____
<i>Computer'</i>	
<i>loggedIn'</i> = $\emptyset$	
<i>users'</i> = $\emptyset$	

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.

<i>AddUser</i>
$\Delta Computer$
$p? : EMPLOYEE$
$p? \notin users$
$users' = users \cup \{p?\}$
$loggedIn' = loggedIn$

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.

<i>RemoveUser</i>
$\Delta Computer$
$p? : EMPLOYEE$
$p? \in users$
$users' = users \setminus \{p?\}$
$p? \notin loggedIn$
$loggedIn' = loggedIn$

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

<i>LogIn</i>
$\Delta Computer$
$p? : EMPLOYEE$
$p? \in users$
$p? \notin loggedIn$
$users' = users$
$loggedIn' = loggedIn \cup \{p?\}$

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.

<i>LogOut</i>	
$\Delta Computer$	
$p? : EMPLOYEE$	
$p? \in users$	
$p? \in loggedIn$	
$users' = users$	
$loggedIn' = loggedIn \setminus \{p?\}$	