Carnegie Mellon University

Software Process Definition – Spring 2002

Homework 01

Paulo Merson

Documentation of an E-Provisioning Process

– **01/28/2002** –

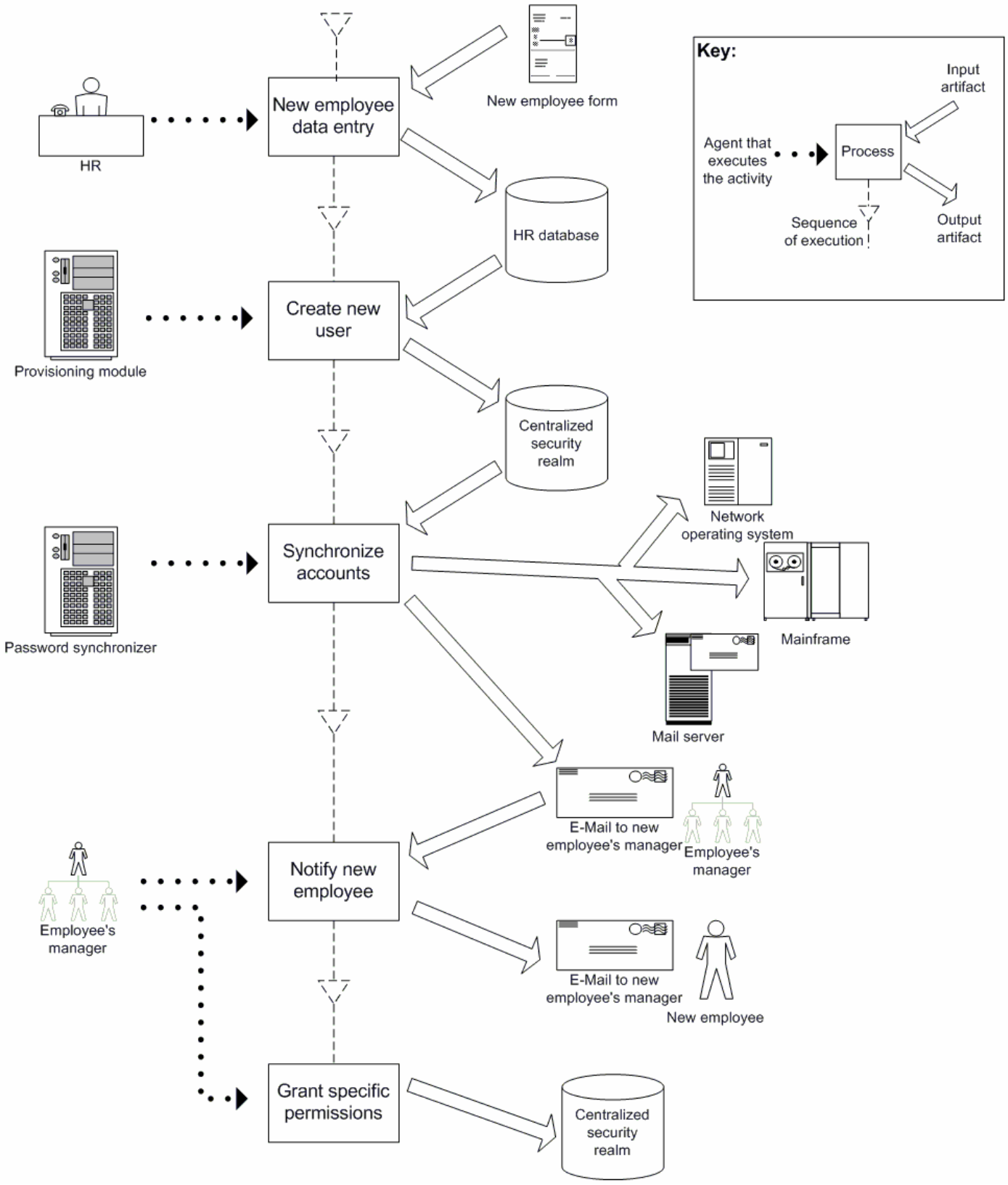
Table of Contents

1 Introduction

The e-Provisioning process starts when a new employee is hired. The objective of the process is to create all user accounts and permissions that this new employee will need in order to perform his or her duties. The process is supported by the access management application that automates most of the work, saving time and not requiring the intervention of network administrators or mainframe operators.

The *Process Model* depicts graphically the sequence of activities, agents, and artifacts within the process. The *Process Definition* provides the details about artifacts, agents and activities.

2 Process Model



3 Process Definition

3.1 Artifacts

Input

- ***New employee form***: This is a form filled up by the new employee that is kept in his/her personal file within the HR department, along with the contract, non-disclosure agreement, and other documents.

Output

- ***E-mail to new employee's manager***: This is a confidential e-mail message automatically generated by the system that contains the user accounts and passwords, e-mail address and home directory pathname. This message is sent to the immediate superior of the employee, which is responsible for handing it to him/her. If the immediate superior is out on vacation or is not working for any reason, then the e-mail is sent to the substitute or the next person in the hierarchy.
- ***User accounts***: As an output of the process, new user accounts are created for the new employee in different environments. The same user name and password is used (single sign-on) to create accounts in:
    - Centralized Security Realm: Used to authenticate the access to all applications.
    - Network Operating System: Used by the user to login to the local network and have access to an individual directory (home directory) in the file server.
    - Mail Server: The employee has an individual account and a personal mailbox.
    - Mainframe: Used to access some corporate applications that still run in the mainframe.
- ***Permissions***: represents that a specific user is granted permission to access applications using specific roles.
- ***Record in HR database***: Consists of the information about the new employee stored in the HR system database. This initial record holds the following data: SSN, name, data of birth, address, phone, dependents, starting date, salary, department, and position.

3.2 Agents

- ***HR***: Person of the Human Resources department responsible for operating the HR system.
- ***Provisioning module***: Program module - part of the access management application - that periodically reads the HR database to identify functional (?) events that should trigger the provisioning process.
- ***Password Synchronizer***: Program module - also part of the access management application - that periodically reads the centralized security realm looking for new user IDs. It has *resource*

adapters that interact with the mainframe system, the network operating system and the mail server to create user accounts in each of these environments.

- ***Employee's manager***: The immediate superior of the new employee in the organization.

3.3 Activities

New employee data entry

Description: This activity is performed by HR. It consists of entering the data of new employee into the HR application. The sub-activities are:

1) Type personal data: SSN, name, data of birth, address, phone, dependents.
2) Type functional data: Starting date, salary, department, position.

Entry criteria: A newly hired employee has signed the contract and filled up the new employee form.

Exit criteria: all data was typed in and the application showed a "New employee created" message.

Input: new employee form filled up.

Output: record in HR database.

Purpose: The event of having a new employee is unknown to all automated systems and computer services until this activity is performed. It's essential because it starts up the tasks necessary to provide to this new employee all computing resources he or she will need to perform his/her duties.

Create new user

Description: This activity is a batch processing performed by the provisioning module every night. It creates a new user account to the new employee and grants access to the applications, storing this information in the centralized security realm. The user name is algorithmically formed by a combination of the first and last name. The sub-activities are:

1) Read HR system database looking for new employees. For each new employee found, do the following tasks.
2) Combine first and last name to create a new user name.
3) Generate a random password.
4) According to the employee position and department, grant the permissions needed to access applications.

Entry criteria: Nightly processing is started and a new employee record is found in the HR system database.

Exit criteria: Execution complete and user accounts and permissions stored in the centralized security realm for all new employees.

Input: record in HR database.

Output: user account in the centralized security realm; permissions inserted in the centralized security realm.

Purpose: Produce a user name that will be used by the employee to access all computing resources in the company and store this information in the centralized security realm.

Synchronize accounts

Description: This activity is performed by the password synchronizer and is executed every night after the execution of the "create new user" activity. It reads the new user in the centralized realm and creates accounts for this new employee in the different platforms or services to which access is required. The sub-activities are:

1) Read centralized security realm looking for new user IDs. For each new user ID found, do the following tasks:
2) Send commands to the network operating system to create user account, create home directory, and grant minimal permissions to directories and other resources the employee will need to access, based on his/her position and department.
3) Send commands to the mainframe to create user account and grant the minimal permissions to mainframe resources the employee will need to access, based on his/her position and department.
4) Send commands to the mail server to create a personal mail box, send "welcome" message with instructions and the policy for use of computing resources in the company, and include the new e-mail address in the necessary mail lists according to the position and department of the new employee.
5) Send an e-mail message to the new employee's manager informing the creating of use accounts and passwords.

Entry criteria: Nightly processing of "create new user" is finished and a new user is found in the centralized security realm.

Exit criteria: Execution complete and user accounts and permissions created within the network operation system, mainframe system, and mail server.

Input: user account in the centralized security realm.

Outputs:

- user account in the network operating system;
- user account in the mainframe system;
- user account in the mail server;
- e-mail to new employee's manager.

Purpose: Create user accounts and permissions that the new employee will need to use the computing resources.

Notify new employee

Description: This activity is performed by the new employee's manager, who must forward the data received about the new employee's accounts to the employee in a secure way. The sub-activities are:

1) Receive e-mail message informing the creation of user accounts for the new employee.
2) Print the e-mail message.

3) Give the printed message directly to the new employee (do not drop it on his/her table, give it to another person, or leave it in his drawer).
4) Delete the e-mail message from the mailbox for security.

Entry criteria: The manager received the e-mail notifying that the new employee already has accounts to access the network.

Exit criteria: The new employee received and read the printed message.

Input: e-mail to new employee's manager.

Output: e-mail to new employee's manager printed and handed to the new employee.

Purpose: The new employee has no access to computing resources until he/she gets a user ID and password. The purpose of this activity is to forward to the employee the information necessary to login and use the network. Ultimately, this final activity gives the employee the key to computing resources needed to do the work in the company.

Grant specific permissions

Description: This activity is performed by the new employee's manager, who must give access to applications that this new employee will use. The sub-activities are:

5) Enter the delegated administration module of the access management application.
6) Select the user name of the new employee.
7) For each application that the employee will need, select the appropriate roles and click "request grant".
8) Wait until the application inform if the request succeeded or was denied.

Entry criteria: The manager received the e-mail notifying that the new employee already has accounts to access the network; or, at any time, the employee needs temporary or permanent access to a different application or role to execute his/her work.

Exit criteria: The system informed the result of all requests.

Input: none.

Output: permissions inserted in the centralized security realm.

Purpose: Each employee within a department may be assigned to different tasks and hence need privileges to execute different operations in the applications available. The purpose is having the manager grant the specific permissions that the employee will need to perform the specific responsibilities he/she was delegated.

4 Glossary

- ***Access management application***: security system that controls the access of users to all computing resources. Different modules handle authentication, authorization, single sign-on, password reset, provisioning, entitlement and rights management, etc. For more, check the documentation of the application.
- ***Home directory***: individual directory on the file server where the user can store his files.
- ***Provisioning***: in the context of this process, provisioning represents the acts necessary to give the new employee all computing resources he/she will need to perform the duties of his/her position. The e-provisioning process is part of a more comprehensive provisioning process that must provide the new employee with other necessary resources, such as an office or cubicle, desk and chair, extension number, badge and keys, desktop computer, etc.
- ***Role***: an application offers various operations and is used by different groups of users. Each group of users may need permissions to execute a different set of operations. A role represents one set of operations that a group may need in an application. For example, the payroll system can have different roles, such as “call-in”, “finance”, “allEmployees”, “hr”, “C-suite”, etc.
- ***Security domain***: same as security realm.
- ***Security realm***: repository of user IDs, keys, passwords, permissions, groups, roles, and other data used to control the access to a resource.