The workforce management case study: functional analysis and access control requirements

Maarten Decat
Jasper Bogaerts
Bert Lagaisse
Wouter Joosen
Report CW 655, February 2014

Katholieke Universiteit Leuven
Department of Computer Science
Celestijnenlaan 200A – B-3001 Heverlee (Belgium)

The workforce management case study: functional analysis and access control requirements

Maarten Decat
Jasper Bogaerts
Bert Lagaisse
Wouter Joosen
Report CW 655, February 2014

Department of Computer Science, K.U.Leuven

Abstract

Software-as-a-Service (SaaS) is a maturing model for offering online applications which is drawing a growing interest from industry. However, SaaS is still facing many challenges which hinder its widespread adoption. One of these challenges is manageable and effective access control in the presence of the multiple organizations involved. The first step to address this challenge is clarifying the requirements for access control for SaaS and the challenges that result from them. To achieve this, we analyzed a case study of a SaaS application in the domain of electronic workforce management. The analysis was performed with the cooperation of the involved company (which is anonymized in this document). This document (i) describes the SaaS application itself, using an illustrative scenario, use cases and textual non-functional requirements and (ii) provides a set of access control policies that apply to this application.

Keywords : C.2.4 [Computer-Communication Networks]: Distributed Systems - Distributed Applications, D.4.6 [Security and Protection]: Access controls.

Contents

List of Figures

1 Introduction

Software-as-a-Service or *SaaS* is a maturing model for offering online applications with a growing interest from industry. Software-as-a-Service (SaaS) is a type of cloud computing in which a tenant organization rents access to a shared, typically web-based application hosted by the provider [1]. For the tenant, SaaS promises the benefits of ease of use and low management costs: employing a SaaS application does not require the tenant to have specialized on-premise IT infrastructure, nor skilled (and expensive) IT personnel. For the provider, SaaS also promises lower management costs by allowing the same application to be utilized by multiple tenants, a concept called multi-tenancy. However, SaaS is still facing many challenges which hinder its widespread adoption. One of these challenges is manageable and effective access control for SaaS applications in the presence of the multiple organizations involved.

Access control is an important part of application-level security that, from a high-level point of view, limits the *actions* a *subject* (e.g., a user) can take on an *object* in the system (e.g., a file). On the one hand, the process of access control can be divided into *authentication* and *authorization*. Authentication confirms the stated identity of a subject, for example by checking that the subject knows the combination of a username and password; authorization subsequently confirms the subject is allowed to do the desired action on the desired object. On the other hand, access control can also be divided into the two main concerns of *management* and *enforcement*. Access control management is generally referred to as *Identity and Access Management* or *IAM*. The management of authentication data is generally referred to as *User Management* or *Identity Management* and its primary purpose is to manage user accounts and their properties. The management of authorization data is generally referred to as *Entitlement Management* and its primary purpose is to manage the rights (or entitlements) of users in the applications of the organization. A user's rights are often not defined explicitly but inferred from declarative *access control policies* which define the rules that constrain the actions of users in an application. Since these policies reason about the properties of users, entitlement management is closely related to identity management. Enforcement of these policies is then externalized into security middleware.

In this document, we investigate the requirements for access control for SaaS by analyzing a case study of a SaaS application in the domain of electronic workforce management. The analysis was performed with the cooperation of the (existing, but anonymized) company eWorkforce. eWorkforce is a one-stop shop for product or service appointments (e.g., install or repair jobs), for which eWorkforce provides the people and handles the workflow planning. Customers can create tasks and the technicians of eWorkforce and the subcontractors receive appointments to be executed using the central eWorkforce application. The complete application is a good example of an application that has to cope with complex business relationships, which results into complex requirements for access control. Instead of describing the system as a whole, this document focuses on one specific scenario for illustrating resulting access control require-

ments.

The rest of this part is structured similarly as the previous part: Section 2 informally describes the illustrative scenario, starting from a basic scenario and gradually adding complexity. Section 3 describes the system from the scenario more formally as use cases. Section 4 briefly lists some important non-functional requirements for the system. Section 5 gives a glossary of the most important terms used in this document. Section 6 elaborates on access control policies that apply to the system in the context the presented scenario. Finally, Section 7 concludes this part.

2 Illustrative scenario

This section illustrates the scope of this case study by describing a specific scenario. We start by describing the basic setup of the application and gradually add more complexity.

2.1 Basic scenario

In essence, eWorkforce is a one-stop shop for product or service appointments such as device installs or repairs. The customers of eWorkforce are companies who create work orders for eWorkforce to execute. For example, TelCo (a telecom provider) employs eWorkforce to execute modem, router and digibox installs and repairs in the homes of their private customers, and PowerProtection (a provider of power protection solutions) employs eWorkforce to install and perform regular checks on UPS systems at their business customers. eWorkforce provides these customers with a SaaS application for creating and managing work orders and therefore, these customers are tenants of the application, as illustrated by Figure 1. This document assumes all customers are tenants of the application. Moreover, we employ the term *primary tenants* for the customers, for reasons that will be explained later.

A work order consists of an address, a description of the work to be done and necessary skills and resources. Work orders can be one-time (e.g., a customer of TelCo reports a problem with his home internet connection, for which a helpdesk operator of TelCo schedules a home visit) or recurring (e.g., the UPS systems installed by PowerProtection have to be checked upon yearly). Recurrent work orders are scheduled by maintenance managers or sales managers of the tenant, one-time work orders can also be scheduled by helpdesk operators. Helpdesk operators can also explicitly schedule appointments, which are a special type of one-time work orders. Appointments allow the client to decide on the appropriate day for the technician to visit. Therefore, appointments should be executed on a specific day instead of before a certain deadline. A work order (both one-time and recurrent) can also consist of multiple sub-work orders, which possibly can be executed by different parties. Such work orders are called composite work orders. Most of the work orders are given by customers with fixed contracts with eWorkforce, such as TelCo, but one-time contracts exist as

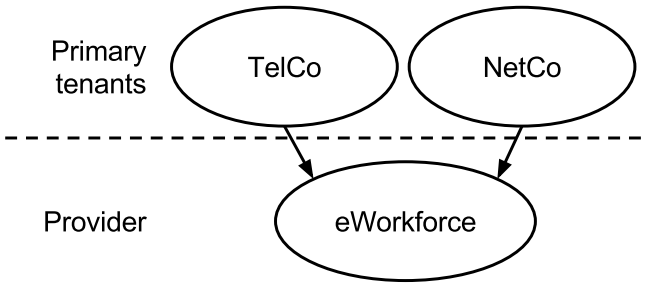

Figure 1: Overview of the basic scenario. Arrows represent customer relationships (e.g., TelCo is a customer of eWorkforce).

well. As an additional constraint, some customers require certified technicians to execute their work orders, e.g., TelCo requires technicians which are trained and certified to work with their products.

In order to execute the work orders, eWorkforce maintains an internal workforce of technicians and an internal warehouse of resources. Workforce managers of eWorkforce maintain the details of the workforce (for example, updating vacation periods, shifts, technician count, technician capabilities etc). After creating a work order, the eWorkforce application assigns tasks to technicians, calculates required resources, appoints transport tasks for these resources and calculates resulting warehouse stocks. During or after executing a task, the technicians report the progress of the task and the consumed resources to the application. The customers can also use the application to check on the status of a certain appointment or update it. The resources stored in the warehouse are provided by the customers, e.g., TelCo provides its branded modems itself, and the customers are contacted in case additional resources are needed. eWorkforce itself is responsible for collecting the new resources from the customer.

Technically, the back-end application is used by end-users as a web application or using a mobile app. The back-end is located in the shared domain of the provider (www.eworkforce.com[1]) and all users are given a tenant-specific client. Possible alternatives are a tenant-specific sub-folder in the provider domain (e.g., www.eworkforce.com/telco), a sub-domain of the organization domain (e.g., appointments.eworkforce.com) or a an tenant-specific sub-domain of the provider domain (e.g., telco.eworkforce.com).

eWorkforce also provides a helpdesk which its tenants can use when they encounter problems with the application. Employees which are responsible for the helpdesk are able to create, edit and remove the work orders for the primary tenants. They are also responsible for handling any questions and issues that the customers of eWorkforce run into.

[1]In reality, the application is located at two domains. For brevity, we only use www.eworkforce.com in this document.

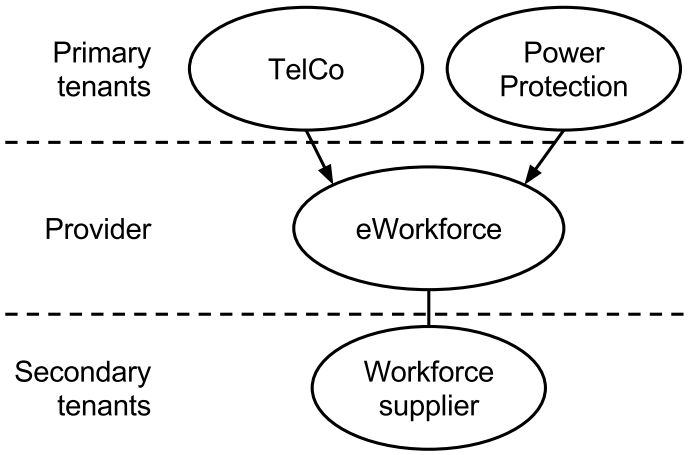

Figure 2: Overview of the basic scenario (see Figure 1) extended with secondary tenants. Arrows represent customer relationships, lines represent business relationships.

2.2 External workforce suppliers

As a first extension to the basic scenario described above, we can take into account external workforce suppliers (see Figure 2). As mentioned above, eWorkforce maintains an internal workforce of technicians. However, eWorkforce also cooperates with external workforce suppliers which provide technicians to which eWorkforce can outsource task execution in order to handle more tasks and increase its scheduling flexibility.

Similar to eWorkforce itself, the workforce suppliers use the application to receive task details and to manage their own workforce. Based on the latter, the scheduling system of eWorkforce assigns appropriate tasks to every workforce supplier. Similarly to the internal technicians of eWorkforce, the technicians of the workforce suppliers can report on the progress of a certain task or the consumed resources during or after the task.

The workforce suppliers are business partners of eWorkforce. Since they use the application for a fundamentally different purpose than the primary tenants (i.e., the customers), we call the business partners the *secondary tenants*. This document assumes that all business partners are tenants of the application.

2.3 External warehouses

As a second extension, we can take into account external warehouses (see Figure 3). As mentioned above, eWorkforce maintains an internal warehouse. However, similarly to the external workforce suppliers, eWorkforce also cooperates with external warehouses next to the internal warehouse. Based on the scheduled appointments, the eWorkforce application schedules resources to be transported from warehouses to the technicians that require them (e.g., “deliver 50

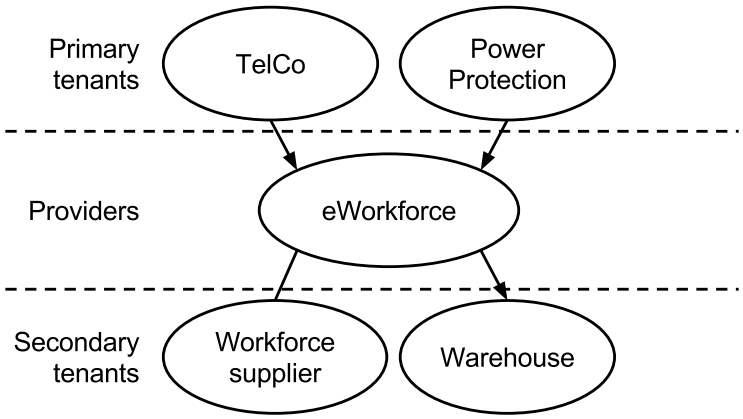

Figure 3: Overview of the previous scenario (see Figure 2) extended with an external warehouse. Arrows represent customer relationships, lines represent business partnerships.

TelCo modems to workforce supplier A by tomorrow morning"), calculates resulting stocks and notifies the customers when the stock in the warehouses need to be refilled. Similar to the internal eWorkforce warehouse, the external warehouses are responsible to collect the resources from the respective customers themselves. To summarize, warehouses use the application to receive stock orders, to update their internal stock number sand to schedule resource collection appointments with customers. Similarly to the workforce providers, the external warehouses are called secondary tenants of the application.

2.4 Subcontractors

As a third extension, we can take into account subcontractors (see Figure 4). Similar to eWorkforce, the external workforce suppliers with which eWorkforce cooperates can outsource tasks to subcontractors themselves. For eWorkforce, the workforce size of a workforce supplier is the sum of its internal workforce size and the workforces of its subcontractors. A workforce supplier should be able to manage the subcontractors it employs next to its internal workforce and each subcontractor should be able to be assigned tasks and manage its internal workforce. Similarly to the previously described technicians, the technicians of the subcontractors can report on the progress of a certain task or the consumed resources during or after the task. Since the subcontractors use the eWorkforce application as the result of their business relationship with a secondary tenant of the application, we call them indirect secondary tenants.

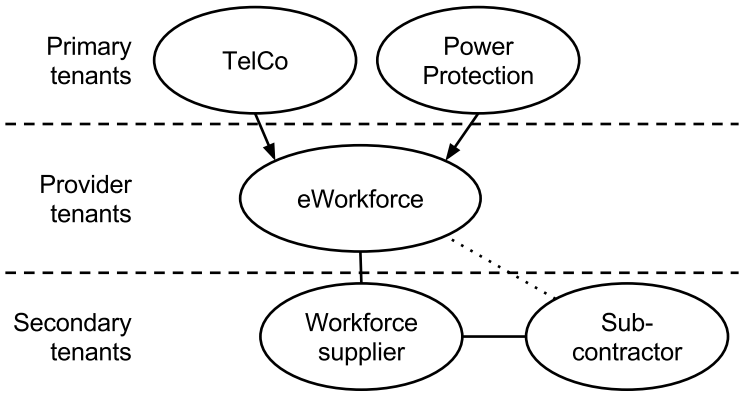

Figure 4: Overview of the previous scenario (see Figure 3) extended with subcontractors. Solid arrows represent a customer relationships, lines represent business partnerships, dotted lines represent indirect business partnerships.

2.5 Helpdesk suppliers

As a fourth extension, we can take into account outsourced helpdesks (see Figure 5). Some of the customers of eWorkforce, e.g., TelCo, do not operate their helpdesk themselves, but (partially) outsource this to a helpdesk supplier. These are not to be confused with the helpdesk of eWorkforce, which handles requests of tenants of eWorkforce.

Since customers of the primary tenants call the helpdesk to report problems, the helpdesk operators of the helpdesk supplier have to be able to create work orders and schedule appointments in the name of primary tenant and check on the status of ongoing work orders. These work orders are limited to one-time work orders. While external workforce suppliers were an example of outsourcing by secondary tenants, an outsourced helpdesk is an example of outsourcing by primary tenants and we call them indirect primary tenants.

2.6 The whole picture

As a summary, we describe the complete set-up as gradually built up in the previous sections (see Figure 6). eWorkforce is the provider of the application central to this document. Primary tenants (i.e., the customers of eWorkforce, e.g., PowerProtection or TelCo) use the application to create, check upon and update work orders (one-time or recurrent) and appointments. The application assigns resulting tasks and appointments to technicians and calculates required resources and resulting warehouse stocks. During or after executing a task, the technicians report the progress of the task and the consumed resources to the application.

eWorkforce provides its own workforce of technicians and its own warehouse, but also cooperates with external workforce suppliers and external warehouse.

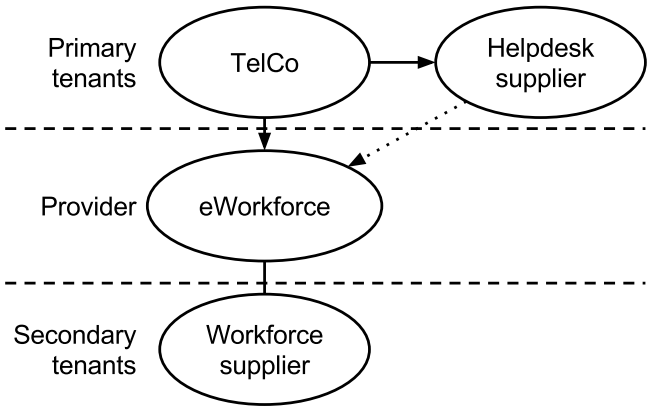

Figure 5: Overview of the previous scenario (see Figure 4) extended with helpdesk suppliers. Solid arrows represent customer relationships, dotted arrows represent indirect customer relationships, lines represent business partnerships.

These business partners are the secondary tenants of the application and use the application in a similar way to the internal workforce and warehouse of eWorkforce.

Both primary and secondary tenants can outsource some of their responsibilities to other companies, e.g., TelCo outsources its helpdesk to a helpdesk supplier and a workforce supplier can outsource task execution to a subcontractor. These companies use the application as the result of their business relationship with a direct tenant and are therefore called indirect primary or secondary tenants. The indirect tenants use the application in a similar way to their respective direct tenants.

3 Functional requirements

Following the illustrative scenario of the previous sections, this section describes the eWorkforce application more formally in the form of use cases and non-functional requirements. The use cases describe the actions which should be controlled by access control, the non-functional requirements apply to the access control sub-system as well. For clarity, we start by giving an overview of all actors and organizations involved in the eWorkforce application.

3.1 Actors

Figure 7 shows the Actor Hierarchy used in describing the functional requirements. Since organizations are an important concept in this case study, we explicitly model them and the relationship between the Actors and the Organizations. For readability reasons, we do not graphically show the relationship between the actor hierarchy and the organization hierarchy in the figure, but

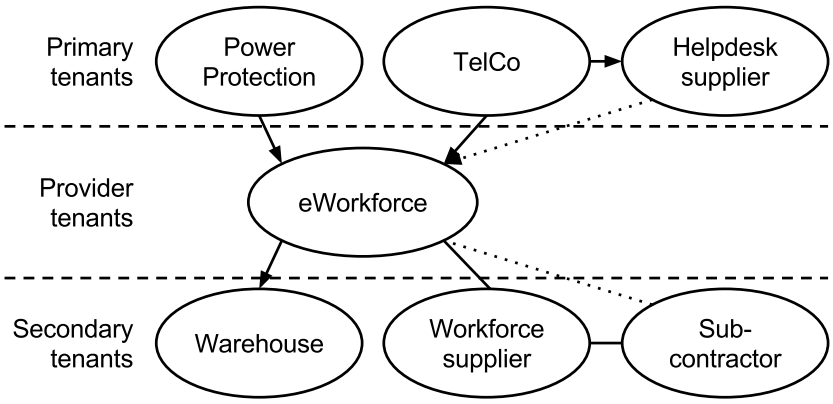

Figure 6: Complete overview of the scenario. Solid arrows represent a customer relationships, dotted arrows represent indirect customer relationships, lines represent business partnerships, dotted lines represent indirect business partnerships.

only describe it in the text below. Note that although an organization technically is not an actor, the term can be used as an abstraction in use cases. For example, the phrase "Warehouse A responds to the request of Tenant B" means "An employee of Warehouse A responds to the request of an employee of Tenant B".

Actors

1. **User**: A general user of the application.
2. **Member**: member of an Organization. Every user of this system is a member of an organization.
3. **Sales Manager**: A User who manages sales for a certain Primary Tenant and uses the application to create and manage work orders and appointments for it. A Sales Manager can create both recurrent and one-time work orders. A Sales Manager is a member of a Primary Tenant.
4. **Maintenance Manager**: A User who manages maintenance jobs for a certain Primary Tenant and uses the application to create and manage work orders and appointments for that Primary Tenant. A Maintenance Manager can create both recurrent and one-time work orders. A Maintenance Manager is a member of a Primary Tenant.
5. **Helpdesk Operator**: A User who operates a helpdesk for a Primary Tenant and uses the application to create and manage work orders and appointments for that Primary Tenant. A Helpdesk Operator can only create one-time work orders. A Helpdesk Operator is a Member of a Helpdesk Provider.

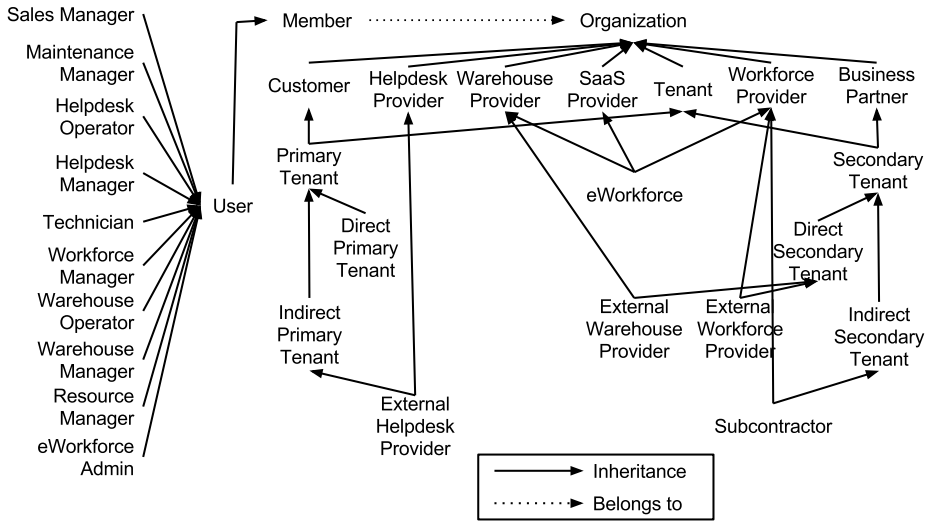

Figure 7: Actor and organization hierarchy.

6. **Helpdesk Manager**: A User who manages a helpdesk and uses the application to manage Helpdesk Operator accounts. A Helpdesk Manager is a Member of a Helpdesk Provider.

7. **Technician**: A User who physically executes work orders and uses the application to receive his/hers assigned tasks and appointments, update the status of these tasks and list used resources. A Technician is a member of a Workforce Provider.

8. **Workforce Manager**: A User who manages the workforce (i.e., Technicians) of an Workforce Provider and uses the application to manage Technician accounts. A Workforce Manager is a member of a Workforce Provider.

9. **Warehouse Operator**: A User who operates a warehouse (i.e., transports resources from and to the warehouse) and uses the application to receive and complete assigned stock requests. A Warehouse Operator is a member of a Warehouse Provider.

10. **Warehouse Manager**: A User who manages a warehouse and uses the application to receive stock requests and assign them to Warehouse Operators. A Warehouse Manager is a member of a Warehouse Provider.

11. **Resource Manager**: A User who manages resources for a certain Primary Tenant and uses the application for receiving resource requests. A Resource Manager is a member of a Primary Tenant.

12. **eWorkforce Admin**: A User who is responsible for adding, removing and configuring access for Tenants and Subtenants. A eWorkforce Admin is a member of eWorkforce.

Organizations

1. **Organization**: a group of people (i.e., the Members of the Organization), e.g., a company.

2. **SaaS Provider**: Organization which maintains a SaaS application and provides it to Tenants.

3. **eWorkforce**: the SaaS provider for this case study. Since eWorkforce also maintains an internal workforce of technicians and warehouse, eWorkforce also acts as a Workforce Provider and a Warehouse Provider. Moreover, eWorkforce has multiple customers and business partners. Members of eWorkforce can be Technicians, Workforce Managers, Warehouse Operators, Warehouse Managers or eWorkforce Admins.

4. **Customer**: a customer of eWorkforce which creates work orders for eWorkforce to execute. Since this document assumes that every Customer of eWorkforce uses the application, every Customer is a Primary Tenant and vice versa.

5. **Business Partner**: a business partner of eWorkforce with which eWorkforce cooperates to achieve better service. Since this document assumes that every Business Partner of eWorkforce uses the application, every Business Partner is a secondary tenant and vice versa.

6. **Tenant**: an Organization which rents access to the application from the Provider. The Members of a Tenant (or at least a part of) are Users of the application.

7. **Warehouse Provider**: an organization which provides a warehouse, i.e., storage room, means of transport, storage operators, transporters etc. Members of a Warehouse Provider can be Warehouse Operators and Warehouse Managers.

8. **Workforce Provider**: an organization which provides a workforce to execute tasks. Members of a Workforce Provider can be Technicians and Workforce Managers.

9. **Primary Tenant**: a Tenant which uses the application to create a work order for eWorkforce to execute. Since this document assumes that every Customer of eWorkforce uses the application, every Customer is a Primary Tenant and vice versa.

10. **Direct Primary Tenant**: a Primary Tenant which is directly related to eWorkforce as a Customer, e.g., TelCo.

11. **Indirect Primary Tenant**: a Primary Tenant which is indirectly related to eWorkforce, i.e., it uses the application as the result of a business relationship with another Primary Tenant, e.g., an External Helpdesk Provider.

12. **Helpdesk Provider**: an organization which provides a helpdesk to its customers, e.g., TelCo. Members of a Helpdesk Provider can be Helpdesk Operators or Helpdesk Managers.

13. **External Helpdesk Provider**: Indirect Primary Tenant to which a Direct Primary Tenant can outsource its helpdesk. Thus, the Helpdesk Operators of the Helpdesk Provider act as Members of this Direct Primary Tenant.

14. **Secondary Tenant**: a Tenant which uses the application to support executing work orders, e.g., receive tasks, input workforce details, input stock details etc. Since this document assumes that every Business Partner of eWorkforce uses the application, every Business Partner is a secondary tenant and vice versa.

15. **Direct Secondary Tenant**: a Secondary Tenant which is directly related to eWorkforce as a Business Partner, e.g., an External Warehouse Provider or External Workforce Provider.

16. **External Warehouse Provider**: a Warehouse Provider employed by eWorkforce to outsource warehousing to. Every External Warehouse Provider is a Direct Secondary Tenant.

17. **External Workforce Provider**: a Workforce Provider employed by eWorkforce to outsource task execution to. Every External Workforce Provider is a Direct Secondary Tenant.

18. **Indirect Secondary Tenant**: a Secondary Tenant which is indirectly related to eWorkforce, i.e., it uses the application as the result of a business relationship with another Secondary Tenant, e.g., a Subcontractor.

19. **Subcontractor**: an External Workforce Provider employed by another External Workforce Provider to outsource task execution to and therefore becomes an Indirect Secondary Tenant. A Subcontractor is an Indirect Secondary Tenant.

3.2 Use Cases

Remarks

These use cases describe only a part of the whole system of eWorkforce. For scoping reasons, we simplify the following:

- Task scheduling: For the sake of brevity of the use cases, we simplify how the system schedules tasks and communicates with end-users. Examples of ignored functionality:
  - Instead of fixing on a single date, a client could provide several dates and time periods in which he/she is available for an appointment, after which the system makes a decision and notifies the client.
  - A client could be notified that the Technician will arrive within thirty minutes as the result of the progress of previous tasks in the Technician's task schedule.
  - Failure of scheduling tasks is not considered in the use cases. Instead, it is assumed that the scheduling of tasks is always successful and a Technician's task schedule can never be overburdened.
  - The use cases assume a Technician can always complete his daily task schedule while in practice it could be the case that a Technician cannot finish the task schedule by the end of the day due to circumstances. In practice, incomplete tasks schedules require task rescheduling, which is supported by the functionality in scope.
  - In case of updates to the daily task schedule of today, a Technician can be notified explicitly. Instead, the use cases assume the Technician checks his schedule after each completed task.
- Transportation of resources: In practice, eWorkforce employs third-party transportation companies (e.g., UPS or DHL) for bringing resources from warehouses to technicians. However, these companies do not use the application and are not tenants of eWorkforce. In order to incorporate this functionality, this document assumes the warehouses themselves provide transport of their resources.
- Warehouses refills: For the sake of brevity, appointments between warehouses and primary tenants to refill the warehouse do not need tenant confirmation. Moreover, similarly to task scheduling, we simplify how the system schedules warehouse refills and for example, do not take into account optimization.

Resulting event flow

For clarity, we first illustrate the complete event flow in scope of this document and described in more details by the use cases. This event flow results from the scenario above and the simplifications described in the previous section.

Work order flow:

- A maintenance manager, sales manager of helpdesk operator creates a work order (one-time or recurrent) or appointment. An appointment should be executed on a fixed date, other work orders before a certain deadline.

- The System schedules the open work orders into a daily schedule for each Technician so that (i) appointments are executed on their fixed day and other work orders are executed before their deadline, thereby taking into account the Technician's availability and capabilities and (ii) the total travel distance and executing time are minimized.
- Technicians check their daily task schedule at the start of every day and after each completed task and can optionally view future (and therefore tentative) daily schedules.
- After each task, the technicians mark the task as completed and indicate consumed resources. This way, the system can calculate the available resources for each technician. It is assumed that a technician can always complete each task on his daily schedule.

Resource flow:

- Based on the task schedule of each technician, the system calculates the required resources for each technician.
  - If each technician disposes of sufficient resources to execute its assigned tasks, no further action is required.
  - If a technician does not dispose of sufficient resources to execute its daily schedule, the system looks for a warehouse holding the required resources.
    - If such a warehouse is found, the system sends a resource request to the warehouse stating which resources are to be transported to which Technician by which date. More precisely, a warehouse manager at the warehouse will receive the resource request and will instruct an operator to fulfill it. This is not handled by the application.
    - If no such warehouse can be found, the system sends (i) a stock refill request to a warehouse which can hold the required resources stating which resources are to be fetched from which primary tenant by which date and (ii) a notification to a resource manager at that primary tenant that the resources will be fetched. Again, the request is received by a warehouse manager and fulfilled by an operator, but this is not handled by the application. Afterwards, the warehouse manager marks the request as completed and the system deduces the new stock levels of the warehouse.

Optionally, the stock levels of a warehouse can be manually updated by a warehouse manager.

3.2.1 UC1: Log in

- Summary: A User wants to use the application and logs in by providing authentication credentials.
- Primary actor: User
- Preconditions:
- Postconditions:
  - The Primary Actor is authenticated and can use the application.
- Main scenario:
  1. The Primary Actor indicates he wants to log in to the application.
  2. The Primary Actor provides authentication credentials, e.g., username and password.
  3. The System checks the provided authentication credentials.
  4. The System confirms successful authentication to the Primary Actor and logs him in, e.g., by setting a cookie.
- Alternative scenario:

  4b. The provided credentials are incorrect. The System notifies the Primary Actor of this. Restart from step 2.
- Remarks:
  - This use case does not take into account which method of authentication is used (cfr. step 2 and 3). For example, authentication can be done locally with eWorkforce or with a third party using a technique such as username-password, security tokes, IP-based etc.

3.2.2 UC2: Log out

- Summary: A logged in User signs out of the application
- Primary actor: User
- Preconditions:
  - The Primary Actor is logged in.
- Postconditions:
  - The Primary Actor is logged out and cannot use the application any more without logging in again.

- Main scenario:

  1. The Primary Actor indicates he wants to log out of the application.
  2. The System logs the Primary Actor out.
  3. The System indicates success to the Primary Actor.

3.2.3 UC3: Create work order

- Summary: A User creates a work order to be executed by eWorkforce.
- Primary actor: Sales Manager, Maintenance Manager, Helpdesk Operator
- Abstract use case: implemented by UC4: Create One-Time Work Order and UC5: Create Recurrent Work Order.
- Preconditions:
  - The Primary Actor is authenticated.
- Postconditions:
  - A work order is created for the Primary Actor.
  - The System has recalculated tasks and resources.
- Main scenario:

  1. The Primary Actor indicates he/she wants to create a work order.
  2. If this work order is a composite work order, the Primary Actor provides an address, a description of the work to be done and the number of sub-work orders. For each sub-work order: Include UC3: Create work order. If this work order is a simple work order, the Primary Actor provides an address, a description of the work to be done and necessary skills and resources.
  3. The System checks the validity of the given information.
  4. The System creates a new work order with the given information.
  5. The System indicates success to the Primary Actor.
  6. The System recalculates tasks and resources: Include UC6: Calculate tasks and resources.

- Alternative scenario:

  3a. The given information was not valid. The System indicates this to the Primary Actor. Continue with step 1.

3.2.4 UC4: Create One-Time Work Order

- Summary: A User creates a one-time work order to be executed by eWorkforce.
- Primary actor: Sales Manager, Maintenance Manager, Helpdesk Operator
- Implements: UC3: Create Work Order
- Preconditions: Identical to UC3: Create Work Order
- Postconditions: Identical to UC3: Create Work Order
- Main scenario:
    1. Extend Step 2 of UC3: Create Work Order: The Primary Actor also provides the deadline of the one-time work order.

3.2.5 UC5: Create Recurrent Work Order

- Summary: A User creates a recurrent work order to be executed by eWorkforce.
- Primary actor: Sales Manager, Maintenance Manager
- Implements: UC3: Create Work Order
- Preconditions: Identical to UC3: Create Work Order
- Postconditions: Identical to UC3: Create Work Order
- Main scenario:
    1. Extend Step 2 of UC3: Create Work Order: The Primary Actor also provides the period of the recurrent work order (e.g., "execute monthly"), together with the periodic deadline.

3.2.6 UC6: Calculate tasks and resources

- Summary: After new data has been added (e.g., creation of a work order, update of workforce details etc), the System (re)calculates tasks and resources and notifies Users of important changes.
- Primary actor: User
- Preconditions:
    - A new work order has been created (UC3: Create work order) or
    - a work order has been updated (UC10: Update Work Order) or
    - workforce details have been updated and there is at least one work order in the System (UC14: Manage workforce).

- Postconditions:
  - A new optimized task schedule is calculated for and given to each Technician.
  - The required resource requests and warehouse refill requests are sent.
- Main scenario:
  1. The System schedules the open work orders into a daily schedule for each Technician so that (i) appointments are executed on their fixed day and other work orders are executed before their deadline, thereby taking into account the Technician's availability and capabilities and (ii) the total travel distance and executing time are minimized.
  2. Based on the task schedule of each Technician, the System calculates required resources.
     (a) If each Technician disposes of sufficient resources to execute its assigned tasks, no further action is required.
     (b) If a Technician does not dispose of sufficient resources to execute its daily schedule, the System looks for a Warehouse holding the required resources.
        i. If such a Warehouse is found, the System sends a resource request to the Warehouse stating which resources are to be transported to which Technician by which date. Include UC16: Send resource request.
        ii. If no such Warehouse can be found, the System sends a stock refill request to a Warehouse which can hold the required resources stating which resources are to be fetched from which Primary Tenant by which date. Include UC18: Send stock refill request.

3.2.7 UC7: Search Work Orders

- Summary: A User searches for work orders matching certain criteria.
- Primary actor: Maintenance Manager, Sales Manager, Helpdesk Operator
- Preconditions:
  - The Primary Actor is authenticated.
- Postconditions:
  - The Primary Actor has received a list of all work orders that match the provided criteria and to which he/she has access.
- Main scenario:

1. The Primary Actor provides the System with criteria that are used to search for specific work orders. He/she can search among the following criteria: address, keywords to be matched in a description, period between which the deadline of the work order occurs and necessary skills and resources.
2. The System shows a list of all work orders that match the provided criteria and to which the Primary Actor has access.
3. The Primary Actor can select a work order to view its details. Include UC9: View Work Order.

3.2.8 UC8: View Work Orders

- Summary: A User views all work orders.
- Primary actor: Maintenance Manager, Sales Manager, Helpdesk Operator
- Preconditions:
  - The Primary Actor is authenticated.
- Postconditions:
  - The Primary Actor has received a list of all work orders to which he/she has access.
- Main scenario:
  1. The Primary Actor indicates he/she wants to view all work orders.
  2. The System shows a list of all work orders to which the Primary Actor has access rights.
- Alternative scenarios:
  3. The Primary Actor selects a work order to view its details. Include UC9: View Work Order.

3.2.9 UC9: View Work Order

- Summary: A User views the details (e.g., status) of a certain work order.
- Primary actor: Maintenance Manager, Sales Manager, Helpdesk Operator
- Preconditions:
  - The Primary Actor is authenticated.
  - The Primary Actor has indicated that he/she wants to view a certain work order, e.g., by selecting the work order at the end of UC8: View Work Orders or UC7: Search Work Orders.

- Postconditions:
  - The Primary Actor has viewed the details of a work order.
- Main scenario:
  1. The System shows the details of the requested work order to the Primary Actor:
     (a) the address,
     (b) the description of the work to be done,
     (c) the necessary skills and resources,
     (d) the deadline (in case of a one-time work order) or the period (in case of a recurrent work order),
     (e) the name and description of the assigned Technician and
     (f) the date on which the work order is scheduled to be executed.
- Alternative scenarios:

  2a. The Primary Actor indicates he/she wants to update the work order. Include UC10: Update Work Order.

  2b. The Primary Actor indicates he/she wants to view a certain task that was scheduled for the work order.

3.2.10 UC10: Update Work Order

- Summary: A User updates the details (e.g., status) of a certain work order.
- Primary actor: Maintenance Manager, Sales Manager, Helpdesk Operator
- Preconditions:
  - The Primary Actor is authenticated.
  - The Primary Actor has indicated that he/she wants to update a certain work order at the end of UC9: View Work Order.
- Postconditions:
  - The Primary Actor has updated the details of a work order.
  - The System has recalculated tasks and resources.
- Main scenario:
  1. The System shows the current values of the editable properties of the requested work order:
     (a) the address,

(b) the description of the work to be done,
(c) the necessary skills and resources,
(d) the deadline (in case of a one-time work order) or the period (in case of a recurrent work order).

2. The Primary Actor provides the new values of these properties of the work order.
3. The System checks the validity of the given values.
4. The System stores the updated work order.
5. The System recalculates tasks and resources: Include UC6: Calculate tasks and resources.

- Alternative scenario:

4a. The given values were not valid. The System indicates this to the Primary Actor. Continue with step 1.

3.2.11 UC11: View daily task schedule

- Summary: A Technician views his/her task schedule for today.
- Primary actor: Technician
- Preconditions:
  - The Primary Actor is authenticated.
- Postconditions:
  - The Primary Actor has viewed his/her task schedule for today.
- Main scenario:

1. The Primary Actor indicates that he/she wants to view his/her task schedule for today.
2. The System shows a list of all tasks that were assigned to the Primary Actor in the order they should be executed and the current/next task first.

- Alternative scenarios:

3. The Primary Actor selects a task to view its details. Include UC12: View task.

3.2.12 UC12: View task

- Summary: A Technician views the details of a task assigned to him/her.
- Primary actor: Technician
- Preconditions:
  - The Primary Actor is authenticated.
  - The Primary Actor has indicated that he/she wants to view a certain task, e.g., by selecting the task at the end of UC11: View daily task schedule.
- Postconditions:
  - The Primary Actor has received the details of the requested task.
- Main scenario:
  1. The System shows the details of the requested task:
     (a) the address,
     (b) the description of the task,
     (c) the date the task is to be executed,
     (d) the progress of the task,
     (e) the estimated resources,
     (f) the resources consumed so far.
- Alternative scenario:
  2. The Primary Actor indicates he wants to mark a certain task as completed. Include UC13: Complete task.

3.2.13 UC13: Complete task

- Summary: After executing a certain task, a Technician indicates the task is completed and indicates the consumed resources.
- Primary actor: Technician
- Preconditions:
  - The Primary Actor is authenticated.
  - The Primary Actor has indicated that he/she wants to mark a certain as completed task at the end of UC12: View task.
- Postconditions:
  - The System has marked the task as completed.

- The System has recalculated resources.

- Main scenario:

  1. The Primary Actor indicates he has completed a certain task. He/she can optionally also provide a report of the fulfilled task (encountered problems, pointers for follow-up, etc.).
  2. The Primary Actor indicates the consumed resources.
  3. The System stores the consumed resources and marks the task as completed.
  4. The System indicates success to the Primary Actor.
  5. The System recalculates resources. Include UC6: Calculate tasks and resources.

- Alternative scenario:

  6. The Primary Actor indicates he wants to see the next task on his daily schedule. Include UC11: View daily task schedule.

3.2.14 UC14: Manage work force

- Summary: A Workforce Manager updates the details of its work force (e.g., the number of workers, their competences (e.g., TelCo certified), their availability (e.g., shifts, sickness) etc).

- Primary actor: Workforce Manager

- Preconditions:

  - The Primary Actor is authenticated.

- Postconditions:

  - The details of the internal workforce are updated.
  - The System has recalculated tasks and resources.

- Note: For brevity, this use case bundles several use cases for managing the internal work force, such as the creation of worker accounts, the assignment of competences to the workers, the update of worker shifts etc.

- Main scenario:

  1. The Primary Actor provides the System with new information regarding the work force. This can be, amongst others, the hiring or firing of a Technician, a change in competences of a Technician (both approval and revocation) or a change in availability (sickness, shifts, leave, etc.).
  2. The System registers the new workforce data.
  3. The System recalculates tasks and resources. Include: UC6: Calculate tasks and resources.

3.2.15 UC15: Manage warehouse stocks

- Summary: A Warehouse Manager updates the details of its internal stocks (i.e., the available resources and their quantity).
- Primary actor: Warehouse Manager
- Preconditions:
  - The Primary Actor is authenticated.
- Postconditions:
  - The details of the internal stocks are updated.
  - The System has recalculated tasks and resources.
- Note: For brevity, this use case bundles several use cases for managing the internal stocks.
- Main scenario:
  1. The Primary Actor provides the list of available resources and their quantity.
  2. The System registers the new stock details.
  3. The System recalculates tasks and resources. Include: UC6: Calculate tasks and resources.

3.2.16 UC16: Send resource request

- Summary: The System sends a request to a Warehouse Operator to transport certain resources held by the corresponding Warehouse to a certain Technician before a certain date.
- Primary actor: Warehouse Operator
- Preconditions:
  - The Primary Actor is authenticated.
  - The System has calculated that a Technician does not hold enough resources to fulfill its future task schedule (UC6: Calculate tasks and resources).
- Postconditions:
  - A resource request is sent to a Warehouse Operator.
  - The Warehouse Operator will transport the specified resources to the specified Technician before the specified date.

- Main scenario:

  1. The System constructs a resource request stating:
     (a) the required resources,
     (b) the Technician to transport the resources to,
     (c) the date by which the resources are needed.
  2. The System sends the resource request to an available Warehouse Operator of a Warehouse holding the required resources.
  3. The Warehouse Operator receives the resource request and will transport the specified resources to the specified Technician before the specified date.

3.2.17 UC17: Complete resource request

- Summary: A Warehouse Operator marks a resource request as completed.
- Primary actor: Warehouse Operator
- Preconditions:
  - The Primary Actor is authenticated.
- Postconditions:
  - The resource request is registered as successful.
- Main scenario:

  1. The Primary Actor has transported the requested resources to the appropriate Technician and indicates that he/she wants to mark the resource request as completed.
  2. The System marks the resource request as completed.
  3. The System updates inventory levels of the involved Technician and Warehouse Provider.

3.2.18 UC18: Send stock refill request

- Summary: The System sends a stock fill request to a Warehouse Provider and notifies the Resource Manager of the Primary Tenant that a stock refill is imminent.
- Primary actor: Warehouse Manager
- Preconditions:
  - The Primary Actor is authenticated.

- Postconditions:
  - A refill request is sent to a Warehouse Manager of a Warehouse Provider.
  - The Resource Manager of the Primary Tenant is notified of the stock refill.
- Main scenario:
  1. The System constructs a stock refill request stating:
     (a) the resource to be refilled,
     (b) the quantity to refill with in order to cope with the imminent appointments and
     (c) a date on which a Warehouse employee will come pick it up.
  2. The System sends the stock refill request to the Warehouse Manager of the Warehouse Provider.
  3. The System sends a notification to the Resource Manager of the involved Primary Tenant, specifying the date and the quantity of resources that will be picked up by the Warehouse Operator.

3.2.19 UC19: View stock refill requests

- Summary: A Warehouse Manager checks views the list of received stock refill requests.
- Primary actor: Warehouse Manager
- Preconditions:
  - The Primary Actor is authenticated.
- Postconditions:
  - The Primary Actor has received a list of received stock refill request notifications.
- Main scenario:
  1. The Primary Actor indicates he/she wants a list of all received stock refill requests.
  2. The System shows a list of all received stock refill requests, indicating which are incomplete, together with the date they were sent, the date for which the refill will take place, the resource that should be collected and the quantity desired.
- Alternative scenario:
  3. The Primary Actor indicates he wants mark a stock refill request as completed. Include UC20: Complete stock refill request.

3.2.20 UC20: Complete stock refill request

- Summary: A Warehouse Manager marks the stock refill request as completed after a Warehouse Operator has collected the resources from the Primary Tenant.
- Primary actor: Warehouse Manager
- Preconditions:
  - The Primary Actor is authenticated.
  - The Primary Actor has indicated that he/she wants to mark a certain stock refill request as completed, e.g., by selecting the stock refill request at the end of UC19: View stock refill requests.
- Postconditions:
  - The stock refill request is marked as completed.
  - The inventory levels are updated.
- Main scenario:
  1. The System marks the stock refill request as completed.
  2. The System calculates and updates the new inventory level of the resource in the Warehouse Provider.
  3. The System indicates success to the Primary Actor.

4 Non-functional requirements

This section describes important non-functional requirements for the system. Again, we focus on the parts of the system related to access control.

- Scalability: The application should be able to handle a lot of appointments involving a lot of resources which are sent by a large number of tenants and their respective subtenants, leading to complex and large tenant hierarchies. Moreover, each of the partner organizations can have a lot of employees using the application. The access control system should therefore scale to large numbers of appointments, resources, tenants, users and requests.
- Performance: The latency of a request to the application should be minimized while maximizing the throughput of requests, especially at peak moments (e.g. when a tenant launches a new product). Since the access control system is involved in every request to the application, these requirements also hold for the access control system.

- Availability: Because the involvement of the access control subsystem in almost every action performed on the application, it is of paramount importance that the subsystem remains highly available in all circumstances. Failure of the subsystem would imply that the whole application is unusable for almost every user.
- Maintainability: The access control system should be able to cope with large numbers of appointments and resources over many tenants and subtenants. In the first place, the access control system should allow self-management for every tenant and subtenant. In the second place, the access control model should provide scalable primitives for expressing these complex requirements.
- Security: The system should be secure. We mainly focus on confidentiality and integrity for all sensitive information of any party in the system, leading to access control requirements. The main example of such sensitive information are the appointments handled by the application, but the access control policies and the data they use can be confidential as well.

5 Glossary

This section describes some of the terminology that will be used in this document to refer to functionality of the application and when describing different scenarios.

- **Appointment**: A one-time work order which is to be executed on a certain fixed date. For example, an appointment can be created by a helpdesk operator when deciding when the technician can visit the client.
- **Business partner**: A company which supports eWorkforce in executing work orders (e.g., workforce suppliers or warehouse suppliers). Business partners are the secondary tenants of the application and use it to manage its workforce, receive assigned tasks etc. Since this document assumes that every business partner of eWorkforce uses the application, every business partner is a secondary tenant and vice versa.
- **Client**: A customer of a primary tenant (a single person or a company). Clients are visited by Technicians to execute tasks at their location (home or company).
- **Composite work orders**: A work order that consists of multiple sub-work orders. For example, for a customer that installs data centers, multiple appointments will be needed for installing the servers, the networking infrastructure, the power supply, the security infrastructure etc. It can even be the case that each of these sub-work orders is executed by another workforce supplier of eWorkforce.

- **Customer**: A company which provides work orders for eWorkforce to execute. Customers are the primary tenants of the application and use it to create and manage work orders. Since this document assumes that every customer of eWorkforce uses the application, every customer is a primary tenant and vice versa.
- **One-time work order**: A work order that does not recur periodically, e.g., a customer of TelCo has reported a problem with his home internet connection.
- **Organization**: An organization is a group of users, possibly involved in the application. Special types of organizations are the provider and the tenants. The expression "an organization uses the application" means the members of the organization use the application and thereby become users of the application.
- **Primary tenant**: A tenant of eWorkforce which uses the application to create work order for eWorkforce to execute. Since this document assumes that every customer of eWorkforce uses the application, every customer is a primary tenant and vice versa.
- **Provider**: the organization that provides the application and manages it. There is only one provider in this application: eWorkforce.
- **Recurrent work order**: A work order that recurs periodically, e.g., PowerProtection provides and installs UPS systems, which have to be checked yearly.
- **Resource request**: A request sent by the system to a Warehouse Provider to transport certain resources to a certain Technician in case that Technician does not have the required resources to fulfill its future daily schedule as calculated by the system.
- **Stock refill request**: A request sent by the system to a Warehouse Provider to refill the stocks of resources of a certain Primary Tenant in case that Warehouse Provider does not have the required resources to fulfill future resource requests as calculated by the system.
- **Secondary tenant**: A tenant of eWorkforce which uses the application to support executing work orders, e.g., receive tasks, input workforce details, input stock details etc. Since this document assumes that every customer of eWorkforce uses the application, every business partner is a secondary tenant and vice versa.
- **Simple work order**: A work order without sub-work orders.
- **Task**: A simple work order assigned to a certain technician. Certain tasks can only be executed by qualified technicians.

- **Task schedule**: The list of tasks to be executed by a Technician. A task schedule is the result of optimally scheduling the tasks for a certain technician to be executed by taking into account their location, the required resources, etc.
- **Technician**: An employee of eWorkforce or a workforce supplier that executes tasks such as maintenance technicians for networks, machines etc or install technicians for modems, machines etc.
- **Tenant**: An organization that rents access to the application from the provider. There are multiple tenants in the application.
- **Warehouse provider**: A business organization which supplies a warehouse, i.e., the space to store resources and the employees to manage it.
- **Work order**: Describes a unit of work to be executed by the technicians of eWorkforce. A work order consists of an address, a description of the work to be done, a deadline and necessary skills and resources. Work orders can be one-time or recurrent. A work order is usually created by a customer of eWorkforce, but the eWorkforce help desk should also be able to create work orders for its customers.
- **Workforce**: The complete group of technicians of eWorkforce or a workforce supplier.
- **Workforce provider**: A business organization which supplies technicians and supporting artifacts (e.g., vans, tools etc) to execute tasks.

6 Policies from the scenario

Following the description of the SaaS application, this section zooms in on the resulting access control requirements. More specifically, this section describes example policies for each organization in the scenario described above. As mentioned before, we are interested in applications which have to cope with complex business relationships amongst the parties that use it. The application should allow each organization to express these access control policies, thereby allowing self-management.For each party we briefly summarize its role in the scenario and list applicable policies.

6.1 General for the application

- Every change in access rights is logged.
- eWorkforce application administrators can access all logs.

6.2 eWorkforce

eWorkforce is the provider of the application. In the first place, eWorkforce manages the application, i.e., creates tenants and subtenants. Additionally, eWorkforce provides a helpdesk for customer support and helpdesk operators should be able to manage work orders for customers. Moreover, some employees of eWorkforce such as the internal warehouse operators also use the application themselves.

Applicable policies

- eWorkforce helpdesk:
  - Only helpdesk operators can create, modify or remove work orders for Primary Tenants.
  - Helpdesk operators can only create, modify or remove work orders that apply to active contracts of a Primary Tenant for which he/she is assigned responsible.
  - All actions done by a helpdesk operator are logged.
  - In case a helpdesk operator tries to create, modify or remove a work order for a Primary Tenant for which he/she is not assigned responsible, the applicable helpdesk manager is notified.
- Application admins:
  - Application admins can create, modify and delete appointments for all tenants of eWorkforce.
  - All actions done by an application admin are logged.
  - Tenants cannot revoke the application admin's access rights to create, modify or delete appointments.
  - Only application admins can create Tenants.
  - All application admins can create Tenants.
  - Only application admins can create subtenants for Tenants.
  - All application admins can create subtenants for Tenants.
- Internal workforce:
  - Only employees of the workforce team can access tasks.
  - Employees can only access tasks of customers which relate to their department (e.g., only members of the UPS department can access tasks created by PowerProtection, which is a UPS supplier).
  - Employees can only access tasks of active projects/contracts.
  - Technicians can only view and complete tasks that are assigned to them.

  - Technicians can only view tasks executed less than one week ago to scheduled less than one week in the future.
  - Workforce Managers can view and complete all tasks assigned to a Technician for which they are assigned responsible.
  - Workforce Managers can only view tasks of two weeks ago to two weeks in the future.

- Internal warehouse:
  - Only warehouse managers can manually update the inventory data of the warehouse.
  - All warehouse managers can manually update the inventory data of the warehouse.
  - All actions done by a warehouse manager or warehouse operator are logged.
  - Inventory data can only be updated on weekdays or on Sunday after 18h00.
  - All warehouse managers can mark a stock refill request sent to the warehouse as completed.
  - A warehouse operator can only view or complete resource requests assigned to him/her.
  - A warehouse manager can view and complete any resource request assigned to any warehouse operator of the warehouse.

6.3 PowerProtection

PowerProtection is an organization that sells and installs uninterruptible power supply (UPS) systems. PowerProtection uses the application to register work orders and schedule appointments and receive stock refill notifications.

Applicable policies

- Sales managers:
  - All sales managers can create work orders.
  - Sales managers can only create one-time work orders.
  - All sales managers can view all work orders.
  - A sales manager can update any work order create by another sales manager.

- Maintenance managers:
  - All maintenance managers can create work orders.

  - Maintenance managers can create one-time and recurrent work orders.
  - Maintenance managers can only create, modify or delete work orders on weekdays.
  - Maintenance managers can only view work orders created by other maintenance managers.
  - A maintenance manager can update any work order create by another maintenance manager.

- Composite work orders:
  - An employee of PowerProtection can view a work order if he/she can view one of its parent work orders.
  - An employee of PowerProtection can update a work order if he/she can view one of its parent work orders.

- Stock refill notifications:
  - Only members of the Provisioning group can receive stock refill notifications.

6.4 TelCo

TelCo is a telecom provider which requires large amounts of resources, technicians, and helpdesk operators in order to successfully connect its clients to their network. TelCo uses the application to register work orders and schedule appointments and receive stock refill notifications.

Applicable policies

- Work orders:
  - Every employee of TelCo which is member of Customer Support can use the application to create work orders.
  - Members of Customer Support which are part of the Company Support group can only send one-time work orders. They can also create recurring work orders if they are Sales Managers or Maintenance Managers.
  - Only Members of Customer Support which are part of the Residential Support group and are Maintenance Managers can create recurring work orders, the rest can only create one-time work orders.
  - Only members of the Repair Support Services group can create work orders which have a deadline which occurs in two days or less.
  - Members of a group can view and update each work order created by another member of that group.

  - Members of a group can view and update any work order created by another member of that group.
  - An employee of TelCo can view a work order if he/she can view one of its parent work order.
  - An employee of TelCo can update a work order if he/she can view one of its parent work order.

- Stock refill notifications:
  - Only members of Technician Support can receive stock refill notifications.
  - All members of Technician Support can receive stock refill notifications.

6.5 Helpdesk Supplier

Helpdesk suppliers provide call center agents which handle all client requests of their customer organizations. They use the application to create, modify or delete work orders on behalf of these customers. Their customer organizations of course need to be tenants of eWorkforce.

Applicable policies

- Helpdesk Operators:
  - All Helpdesk Operators can create a new work order.
  - All Helpdesk Operators can modify a new work order.
  - Work orders can only be created on weekdays from 08h00 to 020h00 and on Saturdays from 09h00 to 17h00.
  - All actions done by a Helpdesk Operator are logged.

- Helpdesk Managers:
  - Helpdesk Managers can only view work orders.
  - Helpdesk Managers can only view work orders created by Helpdesk Operators which are members of the team they are responsible for.

6.6 Workforce Supplier

A workforce supplier is a business partner of eWorkforce that provides the manpower for executing tasks. For example, workforce suppliers might provide Technicians who are trained and certified to perform the installation on behalf of TelCo. Technicians of the workforce supplier use the application to view their daily schedule of assigned work orders and mark them as completed afterwards, workforce manager use the application to update the details of the workforce.

Applicable policies

- General:
  - Only Technicians or Workforce Managers can access tasks.
  - Employees of a Workforce Supplier can only access tasks of customers which relate to their department (e.g., only members of the UPC department can access tasks created by PowerProtection, which is a UPC supplier).
  - Employees of a Workforce Supplier can only access tasks of active projects/contracts.
- Technicians:
  - Technicians can only view and complete tasks that are assigned to them.
  - Technicians can only view tasks executed less than one week ago to scheduled less than one week in the future.
- Workforce Managers:
  - Workforce Managers can view and complete all tasks assigned to a Technician for which they are assigned responsible.
  - Workforce Managers can only view tasks of two weeks ago to two weeks in the future.
- Delegation:
  - Rights to access a task can only be delegated to technicians of the same Workforce Supplier which also have the appropriate certification to also execute them (e.g, only technicians which have a TelCo Certified Technician License may receive tasks on behalf of TelCo) and are active in the region of the client.
  - Technicians can only delegate the right to view a task.
  - Technicians can only delegate the right to access a task which they have been assigned (i.e., delegated tasks cannot be delegated).
  - Workforce Managers can delegate the right to view and complete a task to another technician of the Workforce Supplier.
  - Rights to access a task can only be delegated one week before the task was scheduled to one day after the task was executed.
- Subcontractors:
  - Senior Workforce Managers can view the tasks of subcontractors which relate to their department.

  - Senior Workforce Managers can only view tasks of subcontractors.
  - Subcontractor Managers can view tasks of any subcontractor.
  - Subcontractor employees can only view tasks dispatched by this Workforce Supplier in case the subcontractor still has an active contract.

6.7 Subcontractor

Subcontractors are responsible for handling installation services. They only use the application for viewing tasks that are assigned to them. They consist of one or several technicians which handle installation tasks with the clients of primary tenants of eWorkforce.

Applicable policies

- General:
  - Only Technicians or Workforce Managers can access tasks.
- Technicians:
  - Technicians can only view and complete tasks that are assigned to them.
  - Technicians can only view tasks executed less than one week ago to scheduled less than one week in the future.
  - Employees of a Workforce Supplier can only access tasks of customers which relate to their department (e.g., only members of the UPC department can access tasks created by PowerProtection, which is a UPC supplier).
  - Employees of a Workforce Supplier can only access tasks of active projects/contracts.
- Workforce Managers:
  - Workforce Managers can view and complete all tasks assigned to a Technician in their team.
  - Workforce Managers can only view tasks of two weeks ago to two weeks in the future.

7 Conclusion

Software-as-a-Service or SaaS is a maturing model for offering online applications with a growing interest from industry. While SaaS promises benefits for both users and providers of these applications, the challenge of manageable and effective access control in the presence of the multiple parties involved still hinders its widespread adoption. To address this challenge, the first step is to

clarify the requirements for access control for SaaS. Therefore, we analyzed the SaaS application provided by the company eWorkforce as a realistic case study of such a SaaS application. We started from an illustrative scenario, further specified the application in use cases and non-functional requirements and finally deducted access control policies that apply to this application. Towards the future, this case study can be combined with others in order to identify general requirements for SaaS access control.

References

[1] P. Mell and T. Grance. The NIST definition of cloud computing. *National Institute of Standards and Technology*, 53(6):50, 2009.