Case study
Employee care at an Insurance Company

This paper presents a case study in employee care. One of our customers in employee care is an insurance company ("Insurance Company"), offering employee benefits services such as life insurance, pension plans and healthcare insurance.

The customers of Insurance Company are employers, while the ‘consumers’ of their digital services are the employees of those employer-customers. Employees use Insurance Company’s digital services to view their personal pension statements, update family details and enter insurance claims.

One of first challenges is to limit access for customers to the digital services they subscribed to, while their company may have a complex structure and may evolve. In fact, companies often employ an employee in a local entity and possibly at more than one entity for reasons of cost centre allocation and tax optimisation. Additionally, employers may also come to merge or, conversely, be disentangled.

An additional challenge is to limit access to employee information to those people who are entitled thanks to their role and mandate, thereby respecting the privacy of the employee and GDPR regulations. These people, such as HR managers, team leaders and ombudsmen, may evolve in their career and be put in different roles, move to different entities or be moved out. To respect the privacy, access rights need to follow these movements promptly.
The biggest challenge, however, is; How to provide modern ‘employee care’ that implies a more employee-centric view of the digital services? An employee-centric view enables Insurance Company to digitalise its services and offers apps rather than mailing pension statements and manually processing paper claim forms. Moreover, employee-centric services would extend beyond a single employer. In fact, employees not only change jobs, they may also change employer and may even work for more than one employer at a time. And when an employee leaves for another company, his new employer may be another customer of Insurance Company. With employee-centric services, the employee would expect to be able to access his old records, even if he already left the previous employer.

**Traditional access management**

Payroll services has come to realise that traditional access control models fail. They fail on continued accuracy and on GDPR compliance. Moreover, the complex access administration is failing on scale: having a back office to maintain access for millions of employees and managers who move around is no longer sustainable.

Access management is traditionally implemented using directory-service solutions. Directory-driven solutions may add hierarchical data structures to segregate groups of employees and may layer application permissions on top of this to take subscriptions into account. But hierarchical data and permission structures can’t cope with the complex, ever-changing relationships found at the employers.
Traditional approaches to access management require the back office to be notified of changes at company level, such as business units, organisational structure, relocation, merger, disentanglement, and changes relative to the services subscribed to. And if functionality is added to an existing service or a new service is rolled out, all permissions need to be reviewed.

But it is the movement of employees that may drive access administrators cray: how to deal with the continuous stream of hires that need to be allocated to a team, promotions, mutations, leavers, temporary assignments, interns, students, etc. And yet, the employee may still not have a lifetime view on his career because access is constrained at the employer level.

Controlling access to an employee’s record involves the following steps that must be scalable to millions:

- **Authentication**: Insurance Company only allows people who have been positively identified to access their services. This step is typically already implemented and may involve a directory service and/or a customer identity management system. For example, Akamai/Janrain, SAP/Gigya, AWS Cognito or Auth0 offer the scale but not secure access management of the next two steps.

- **Application-level access**: Insurance Company only allows employees of a customer who paid for the subscriptions to access the services. Before engaging miaa Access, this step was implemented inside the applications themselves using a traditional and less flexible security model.

- **Record-level access**: Insurance Company only allows the employee himself and a few designated managers to access relevant parts of his employee-record. Before engaging miaa Access, this step was enforced using static but cumbersome to manage role-driven access control.

**Why change?**

If traditional methods are still in use today, why change? Well, if Insurance Company is transforming its business to become employee-centric and needs the scale of millions of users, traditional methods fail.

miaa Access removes the need to administer permissions and access rights. It introduces a person-driven access administration model (“PDAA”) whereby the actual user is put at the centre. Secondly, miaa Access externalises access decisions, so that all applications no longer need to worry about fine-grained authorisation matrices. miaa Access introduces policy-driven access control (“PDAC”) that decides who gets access to what in real-time using the access policy of Insurance Company and the corresponding employer.

This person-driven administration model is intrinsically super-scalable and perfectly auditable. Because relationships are managed by the users themselves within controlled workflows, the model maintains accuracy at all times. Last but not least, the model fully embraces employee-centricity.

How does this work in practice? The next sections show how users and customers manage their own administration.
A new approach to application-level access

When an employer becomes a new customer, Insurance Company shall set up the employer and its subsidiaries in its CRM. Traditional models would assign the HR manager as the coordinator who asks to load the employees. Subsequently, different applications will send out separately welcome-mails to all staff.

Access to Insurance Company’s digital services is the easy case: even though we see that it remains a challenge for many back office and security administrators, it can be implemented using traditional approaches.

The real challenges, however, is developing employee-centric services and to scale the administration of access to somebody’s private record to millions. Knowing that employees come and go and may move from one unit to another, the challenge grows exponentially.

Using miaa Access, Insurance Company’s CRM will initialise the employer identity and a first user, typically the HR manager. The HR manager can then set up employer-specific policies and structures. The HR manager can also set up subsidiaries, defined as ‘teams’ that have a relationship with the controlling entity and to which employees will later be linked.

Using miaa Access, common policies and subscription access can be defined at employer-company level. The subsidiaries inherit these access rights and are subject to the common policy. The goal of this set-up course is to govern access and is not to duplicate everything that is already managed by the CRM in terms of contacts, billing, legal structures, etc.

The digital subscriptions are represented as a relationship between the employer-customer and a subscription. Using this relationship, miaa Access can then obtain details of the subscription relevant for access control, such as start date, end date, enabled functions, etc.

To enrol all current staff, Insurance Company activates the miaa Access enrolment workflow to send out ‘welcome’ notifications on behalf of the employer-customer.
Say a person called Ann is hired. The HR manager of company-A will define her as new employee. Using the miaa Access enrolment flow, Insurance Company will send a notification to Ann to ‘welcome’ her and sign her up for the employee benefits scheme of company-A.

When Ann accepts the invitation and has given her consent, she can start using Insurance Company’s services as new employee. By accepting the invitation, she also confirms her email address (or mobile phone number) as her preferred interaction channel.

miaa Access manages the workflow of sending out secure invitations, verifying and recording the response and capturing the consent of the new staff member.
Instead of assigning here permissions, miaa Access grants Ann access to Insurance Company’s services using a chain of relationships. First her relationship with the subsidiary, then the relationship between subsidiary and the employer-customer, and then the relationship between the employer-customer and the digital subscriptions.

A new approach to record-level access

While granting access to digital services can be implemented using traditional methods, e.g. directories, granting access to a personal employee-record is the next hurdle. It is often implemented inside the applications using permissions and authorisations. Many back-offices will confirm that it is painful and error prone to manage permissions and authorisations on a scale of millions of employees.

The relationship model of miaa Access makes this a breeze. Out of the box. So, how does it do its magic?

First, miaa’s person-driven access administration (“PDAA”) establishes roles and relations discussed above. Secondly, the decision whether someone has access to Ann’s employee-record within a given context, is determined in real-time on the spot. It is not a permission that has been set statically. It is rather miaa's policy-driven access control (“PDAC”) that takes the access decision in real-time. It applies Insurance Company’s policy and uses the attributes of the user (such as type of employee and employee status) as well as the relationship of that user with the actual employee.

In the case of Ann, some other relations with company-A were previously established so that the HR manager as well as the ombudsman can access to Ann’s employee-record.

The following tables illustrates the dynamic access decisions that can be taken relative to Ann’s employee-record at Insurance Company.

<table>
<thead>
<tr>
<th>Because she is</th>
<th>implies that she can</th>
</tr>
</thead>
<tbody>
<tr>
<td>beneficiary of her records</td>
<td>update her personal details</td>
</tr>
<tr>
<td></td>
<td>view her employee status</td>
</tr>
<tr>
<td></td>
<td>update her family composition</td>
</tr>
<tr>
<td></td>
<td>view her benefits statement</td>
</tr>
<tr>
<td></td>
<td>enter insurance claims</td>
</tr>
</tbody>
</table>

© 2019 miaa Guard NV – all rights reserved.
Because she is
  o HR manager for company-A
implies that she can
  o update her personal details
  o update employee status
  o view benefits statement
  o not view insurance claims

Because he is
  o ombudsman for company-A
implies that he can
  o view her personal details
  o view family composition
  o view benefits statement
  o view insurance claims

Insurance Company and the employer-customer can add more policy rules before access is granted. For example, additional rules for managers ‘must still be employed by company-A’ and ‘must have been 2-factor authenticated’.

The model of miaa Access really comes to live when taking the employee-centricity a step further. Imagine that Insurance Company promotes the addition of family members to the healthcare part. This would allow the husband Guy to issue and manage his own claim after he went to the hospital.

Using the miaa Access invitation workflow, Ann can invite her husband to join her employee-record as ‘beneficiary as spouse’.
After Guy accepts her invitation, miaa PDAC can then grant access to specific parts of Ann’s employee-record, just enough to be able to enter a claim for his hospital visit.

Because he is
- spouse of Ann

implies that he can
- not view her personal details
- not view employee status
- not view Ann’s benefits statement
- enter insurance claims

While miaa Access manages invitation workflows, it also manages de-friending workflows. Imagine Ann wants to divorce from Guy, she can deactivate his ‘is spouse of’ relation with her employee-record. In case she would invite her children, employee-A may have a policy that they can enjoy her healthcare insurance till they are 18 years of age. At that time, the ‘is child of’ relation from her kid to her employee-record still exists, but the rule ‘must be younger than 18 years’ will deny access.

Summary

miaa Access delegates administration to end users. And it does this in a natural, yet controlled way. Its administration model involves ‘state’ whereby state transitions enable intuitive workflows.

miaa Access also enables self-healing workflows such as an expiration workflow (whereby a relation has a limited lifetime) and an exclusion workflow (whereby a relation is deactivated for reasons of unpaid bills, misbehaviour or resignation).

miaa Access greatly simplifies application design by Insurance Company: the developers only need to focus on its core function rather than on managing the ecosystem of employers, managers, team
leaders, employees. In fact, managing the eco-system and deriving access decisions from that eco-
system has proven to be a science in its own right.

To use any other approach—purpose-built or otherwise—is choosing an inferior solution for crucial
technology that has proven its value, manageability and robustness.

miaa Access enables Insurance Company to:

- Handle organisational changes of an employer easily in one place and have them
  automatically affect their entire organisation and their subscriptions to the digital services;
- Formulate access policies using attributes recorded for employees
- Formulate access policies using detailed consents given by employees
- Formulate access policies using the relation of an employee with the employer, including its
  status (hired-but-not-yet-active, hired-and-active, will-retire, has-retired) and its type
  (regular employee, company representative, personnel manager, auditor, etc.)
- Formulate employer-specific authentication rules, e.g. password policy and two-factor
- Formulate employer-specific authorisation rules and workflows, e.g. approval chains,
  employee invitation flows and self-enrolment capabilities
- Build directories of any size—even with tens of millions—that maintain responsive scale
  and that maintain manageability
- Define and maintain any combination of hierarchical and non-hierarchical organizational
  and approval structures

Since miaa Access allows Insurance Company to query relationships in any direction, they can use it
to perform a variety of top-down and bottom-up queries such as:

- Which applications can be accessed by a specific user?
- Which users are permitted to access a specific application?
- Which records (employee benefits statements and family composition) can a specific user
  view, update or delete?
- Given a specific employer, who can modify its profile and employer-specific policy rules?

For Insurance Company, managing multiple changing roles, groups, products and authorisations has
become an increasingly complex task. Traditional directory services and relational databases cannot
handle the size, complexity, connectedness and ever-changing nature of access-management
information.

miaa Access delivers the performance, security, auditability, scalability and maintainability required
by Insurance Company and offers access control decisions in a matter of milliseconds.