employer_scenario

Scenario: Managing Information in Which Employers and Employees Both Have a Stake (Pending)

Submitted by: Eve Maler

Both an employer and their employees might want to impose their own constraints on the sharing of the same employee-related resource. Examples of pieces of information your employer holds that you might want to share with others:

- Employment status (e.g., active or inactive; often needed when you apply for a loan)
- U.S. Internal Revenue Service W-4 (tax withholding) form details (handy for sharing with accountants and investment planners)

Some additional ones listed in the Liberty ID-SIS Employee Profile Service specification:

- Employee ID internal to enterprise
- Date of hire
- Job start date
- Employee type (e.g., part-time or full-time)
- Internal job title
- etc.

The following “user stories” capture the distinctive aspects of this scenario:

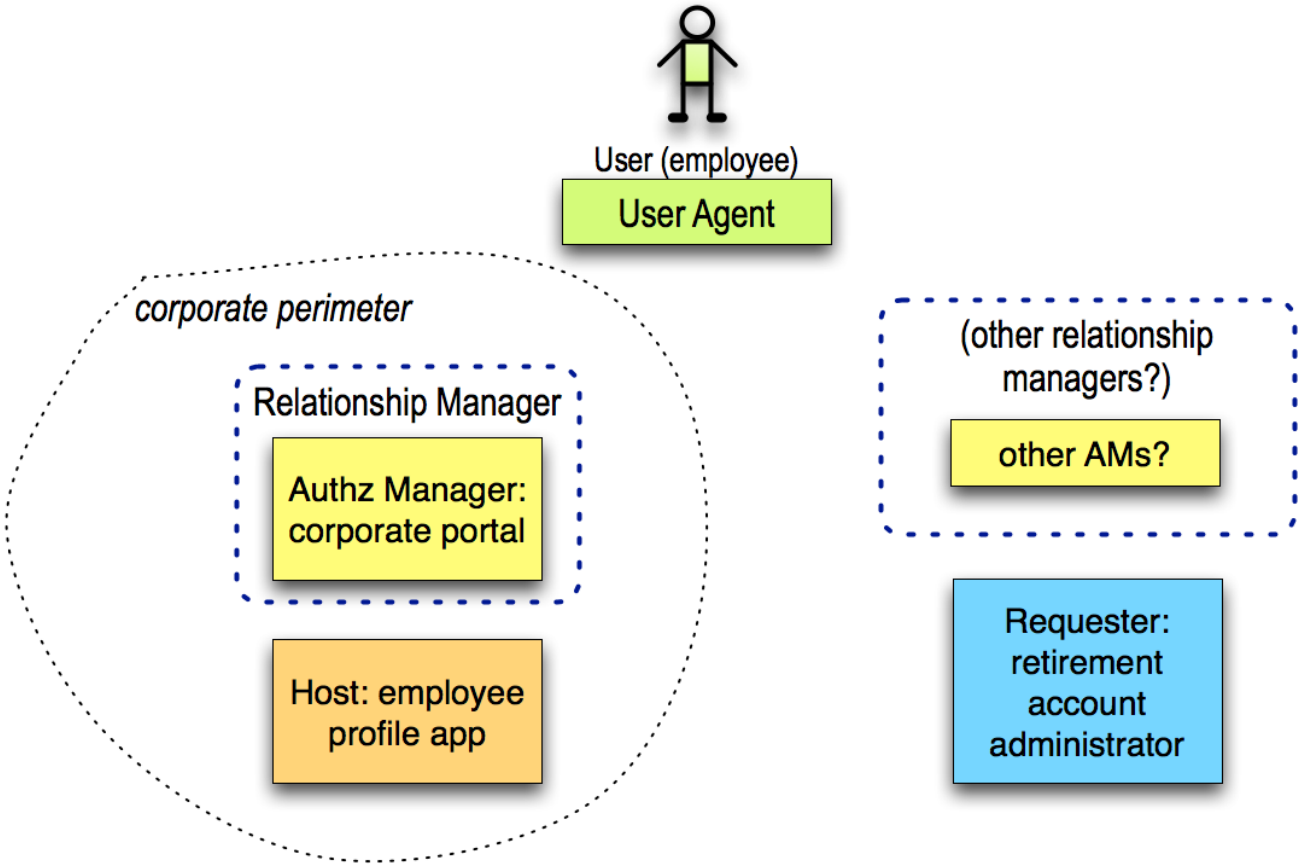
- As an employee, Alice wants to audit and control the further dissemination of information her employer must know about her as a condition of employment.
- As an employer, BigCo wants to adhere to laws and best practices regulating its sharing of information about its employee.

See the use cases below for the different configurations in which the actors might appear.

Issue: In large companies, typically the function of verifying someone's employment is outsourced to a specialized company. The employer is still seen as authoritative for employment status and other such data, though. For such information, where in the use cases below the employer is assumed to be the authoritative Host, perhaps the employer needs to provides a *pointer* to the employer's chosen verification service resource, such that the resource being shared is a pointer to a pointer (double indirection). Or perhaps the employer instructs Alice to introduce her AM to the real Host directly.

Use Case: Employer as AM and Host (Pending)

Submitted by: Eve Maler

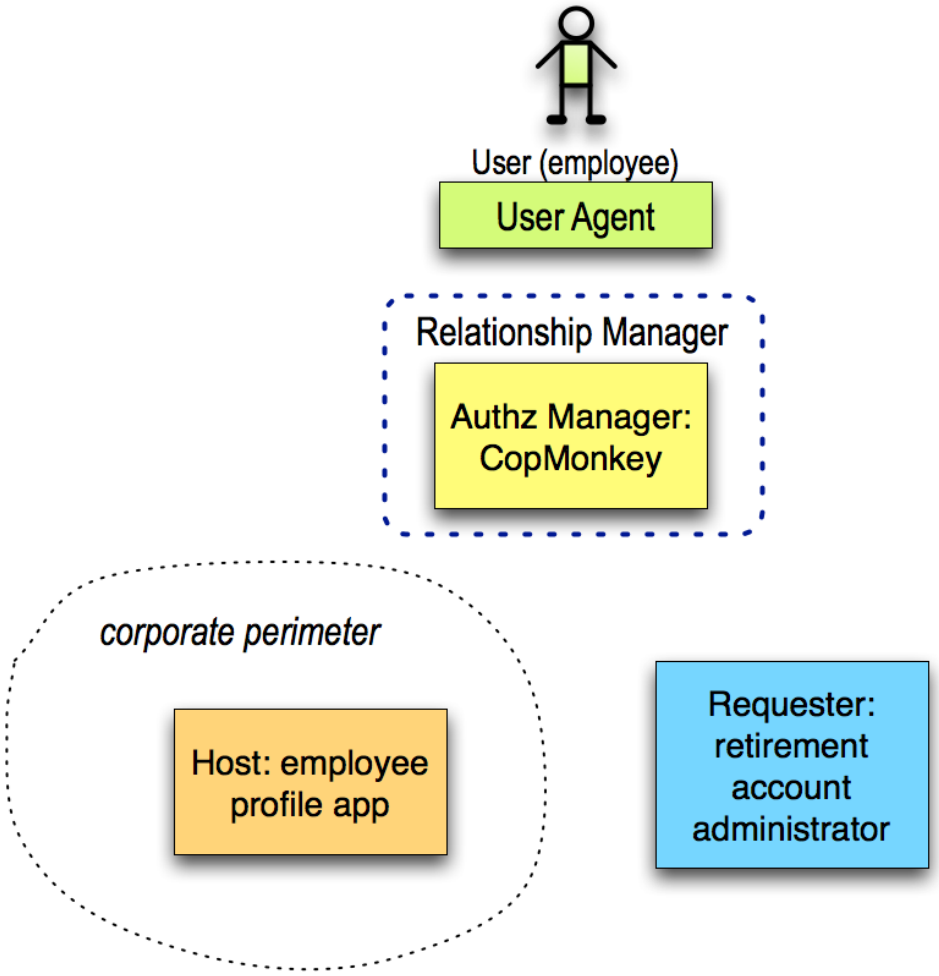


Here, the employer runs an employee profile self-service application that could include both AM and Host functionality. The AM could let Alice configure her sharing policies, but could also let Alice know that it will be enforcing additional constraints out of band with respect to UMA.

This is probably a “legacy” solution because it forces the employee to seek out other relationship managers in the outside world where they’re just an individual rather than an employee, and it seems the employer would be hosting the AM only for corporate inertia (admittedly, a force to be reckoned with).

Use Case: Employer as Host (Pending)

Submitted by: Eve Maler

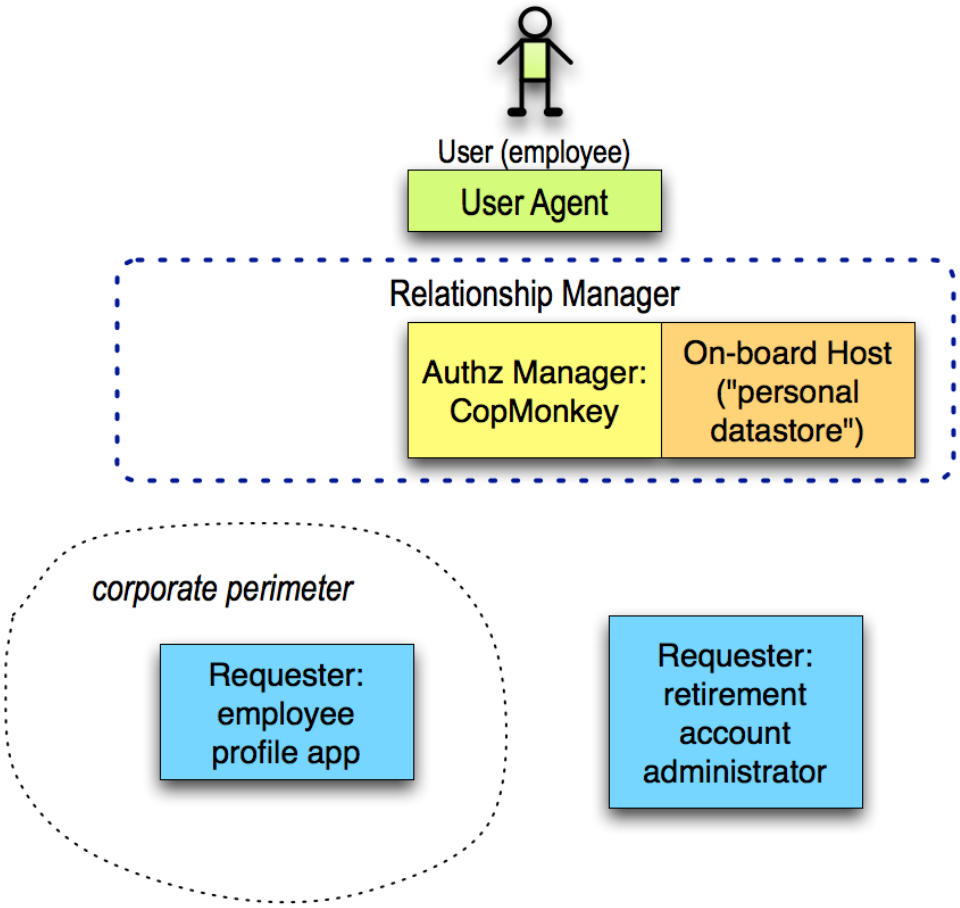


For information for which the employer is authoritative (”Is this person employed here?”), it could offer a Host willing to attest to this on request (in accordance with the instructions issued by Alice's personal AM). If the employer doesn’t want to release the data even though the employee wants to allow the sharing, it could use existing access control mechanisms that are out of band with respect to UMA.

Issue: Should the employer-Host surface a response code to the Requester that reflects this type of refusal? Should it provide audit-log data back to the AM?

Use Case: Employer as Requester (Pending)

Submitted by: Eve Maler



For information that Alice already self-asserts to the employer (”What is the employee’s home address of record?”), the employer should ideally consume this data in the same way some other “vendor” (online service) on the open Internet could. If the employee moves, a number of workflow actions have to unroll on the employer’s side as they would have anyway (in the U.S., moving to a different state might involve withholding a different amount of state income tax), but this is already handled in existing systems when the employee provisions the new information into employee profile apps by value. An on-board “personal datastore” Host is shown here with the user’s chosen AM, but the Host could just as easily be remote.