custodian_scenario

Scenario: Delegating Access Management to Custodians (Pending)

Submitted by: Maciej Machulak

Social applications become increasingly important for a large part of the society. Young and mature Internet users participate in social networks and exchange information about their personal or professional activities. They create connections with friends or other professionals. They share their personal information and digital content using various social applications.

Young people, in particular, have little knowledge about technical complexities of those applications. They have little understanding about the value of information that they submit and share among their peers and other users of those applications. Personal information such as age, sex, telephone numbers or hobbies is often not perceived as valuable. Similarly, other digital content such as photos, short video clips or documents is viewed as any other information which can be freely available for other users of social networks.

In reality, information submitted by users of social networks may be of great value to third parties. Personal information is often used for advertising purposes or can be abused by malicious users for other purposes. Digital content, on the other hand, has influence on how a particular individual is perceived by others, be it employers or peers. As such, restricting access to information and ensuring one's privacy is a necessity.
Younger users of social networking applications may not be aware of the above mentioned security and privacy issues related to the information that they submit. As such, they may expose too much information, which is not desirable. It is often the case that information is shared only with members with whom a person has a direct connection in a social network. However, to increase popularity by having many so-called friends, many users of those applications make connections with others even if they do not know them in person.

To prevent information leakage, parents often require having insight into what information is submitted and shared. They can then restrict publishing of sensitive information. In order to be able to control information, parents need to be given usernames and passwords. This, however, is often perceived to be too intrusive from the perspective of younger users.

In this scenario we discuss how User-Managed Access can be used to support parents with restricting information publishing by their children. We present how younger users of social networking applications can benefit from our proposal. With our scenario we show how the User-Managed Access approach allows a user to delegate access control related tasks to other entities that may have a better understanding of security requirements for resources owned by those users.

Desired Improvements

- Would it be possible for Alice not to be concerned with security and privacy issues and only take care of publishing here data on her favorite social networking application?
- Can Alice achieve that without revealing her username and password to the entity which should have access to her privacy and security settings?
    - The Social Networking Application may allow users to add accounts which could be used to control security and privacy of data published by those users (e.g. Alice may create an additional account with a different username and password which she can hand over to her father – this account could be used by her father to change security and privacy settings for Alice). This approach, however, is not efficient. If Alice uses more than one Social Networking Application then she might need to create multiple accounts and she will end up having security and privacy settings hosted in multiple places).
- Could Alice allow the Social Networking Application to delegate access control related tasks to a third party component? Can such component be under control of a different entity than Alice? Could such entity define arbitrary terms that must be met in order to access Alice's Web resources hosted by her Social Networking Application?

Improved Scenario

Alice, a 14 year old girl, wants to have an account on a popular social networking application - FaceSpace. She wants to create a network of her friends with whom she wants to share photos and discuss her hobbies. She wants to keep in touch with them and does not want to be left behind with new technologies that have been used by her peers for some time now.

When Alice sets up the account at FaceSpace she needs to provide a variety of information. This includes providing information about her age. When Alice states that she's 14 then then FaceSpace detects that she is very young and informs her that she will need parental control over all the information that she submits and wishes to share with other users of the application. What this means is that an adult (legal guardian) will be able to restrict access control for information that Alice submits. However, Alice will still be able to share information if her access control rules do not contradict with those specified by her legal guardian. To set up the parental control, Alice asks her father Bob for some help.

Bob is happy that his daughter will be able to communicate with her friends but he is concerned with what information will be released and how this information might be used by legitimate or malicious users. He knows that FaceSpace has been certified to support parental control and allows third party UMA-based access control systems to be used for that purpose.

Bob is already using a specialized Authorization Manager – CopMonkey – for his own purposes. He uses this AM to define access control policies for his personal data (home address, telephone number) so that he can point other Web services to pull such data as required (e.g. during registration process at different Web sites). Moreover, he protects his online calendar service using CopMonkey and he established necessary relationships between his calendar feeds and his Visa payment service. He wants to be sure that Visa knows where Bob is and can correlate such data with data regarding his credit and debit card usage.

Bob decides that CopMonkey will be perfect for parental control over Alice's information. Therefore, he introduces this AM to FaceSpace (establishes a trust relationship between these two services). As such, he is able to restrict how different information published by his daughter is accessed by her friends or other users of the application. Bob sets up basic policies regarding sharing of such information:
(1) Alice's pictures and video clips can be shared with her friends only.
(2) If the request to either a picture or a video clip comes from a user who does not have a connection with Alice but is a member of the same group as Alice is then such user needs to agree not to further share this picture. Moreover, he needs to provide a certified claim that he is a member of a particular group.
(3) Only friends of Alice can see her personal information such as telephone number or email address.

When the account is set up and parental control has been configured then Alice is able to use FaceSpace just as any other user. She writes comments about her day, posts links to interesting movies. Additionally, she uploads some of her photos and short video clips. She knows that her father is very concerned with Alice's safety and the privacy of her information and that her sharing options are therefore limited. She knows that she can share the information by herself but that she cannot override higher level sharing constraints imposed by her father.
She’s not sure how that works but leaves this issue to her father – after all he is more proficient in defining correct privacy and security settings than she is.

Alice uploads a photo from her birthday party and wishes to share it with some of the users of FaceSpace. When the upload is finished, she clicks on the “Share” link next to the photo and defines the users with whom the picture should be shared. Her sharing options include all of her friends and members of one of the groups that Alice participates in - "Youth Sport". She confirms her sharing choice by clicking on the "Apply Sharing Options" link.

Jane, one of Alice’s best friends, heard that a new photo from a birthday party has been uploaded and wishes to see it immediately. She logs in to FaceSpace and clicks on the Alice’s photo album link. She can see a link to the newly uploaded photo. When she clicks the link, the application detects that a request has been made to an UMA protected resource. Therefore, such access request is subject to access control by the configured Authorization Manager apart from the internal mechanisms used at FaceSpace. Jane knows nothing about UMA and does not see the underlying protocol that is being executed by FaceSpace. She is not aware of the fact that FaceSpace acting on her behalf obtains an access token from Bob's CopMonkey (meeting requirements of policy no. 1). She observes a very small delay before accessing the photo. This delay, however, is visible only when she wishes to access the photo for the first time.

Patrick does not have a connection with Alice but is a member of the "Youth sport" group. He saw that a new picture has been uploaded by one of the group members. Therefore, he clicks on a link to see the photo. Similarly to Jane's case, FaceSpace detects that a request has been made to an UMA protected resource. Therefore, such access request is subject to access control by the configured Authorization Manager apart from the internal mechanisms used at FaceSpace. Patrick gets redirected to a page presenting a short description of what just happened (i.e. that he is subject to additional access control mechanisms as defined in policy no. 2). He sees that he must agree not to distribute the photo and that is a member of the "Youth sport" group. He agrees to that happily and is redirected back to the photo hosted by FaceSpace. Just as Jane, he is not aware of any complexities of the UMA protocol and only knows that he had to agree to some simple terms. Thanks to the UMA protocol, CopMonkey collects the following claims: (a) one self-asserted by Patrick that he will not share a photo, (b) a claim certified by FaceSpace that Patrick is a member of the "Youth sport" group. Both claims are required to authorize FaceSpace access Alice's photo on behalf of Patrick.

Patrick likes the photo very much and he decides to see who Alice is. Therefore, he clicks on her "Profile" link. This access request is also subject to parental control configured for FaceSpace. In this case, Patrick is denied access which conforms to Bob's policy no. 3.

Over time, Alice learns that allowing her father to have impact on security of the resources that she shares with her friends is not a bad thing. She feels safe and knows that everything she submits to FaceSpace is secure. Over time, Alice also learns more about security and sees what information is prevented from being shared with her friends. In the future she hopes to make better security decisions by herself. At some point she'll be fully responsible for controlling access to her resources.

Her father Bob is also happy as he knows that his daughter can communicate with her friends in a safe and secure way. He checks his Authorization Manager on a daily basis and composes access control policies and defines terms as new photos and other resources are uploaded by his daughter. Moreover, he audits all access requests and sees how Alice's friends access her photos and video clips. He hasn't noticed any abuses and is confident in whatever her daughter does. After all, he's fully responsible for her privacy and security and he puts much effort into ensuring that his daughter stays safe and still enjoys the benefits of social networking on the Web.

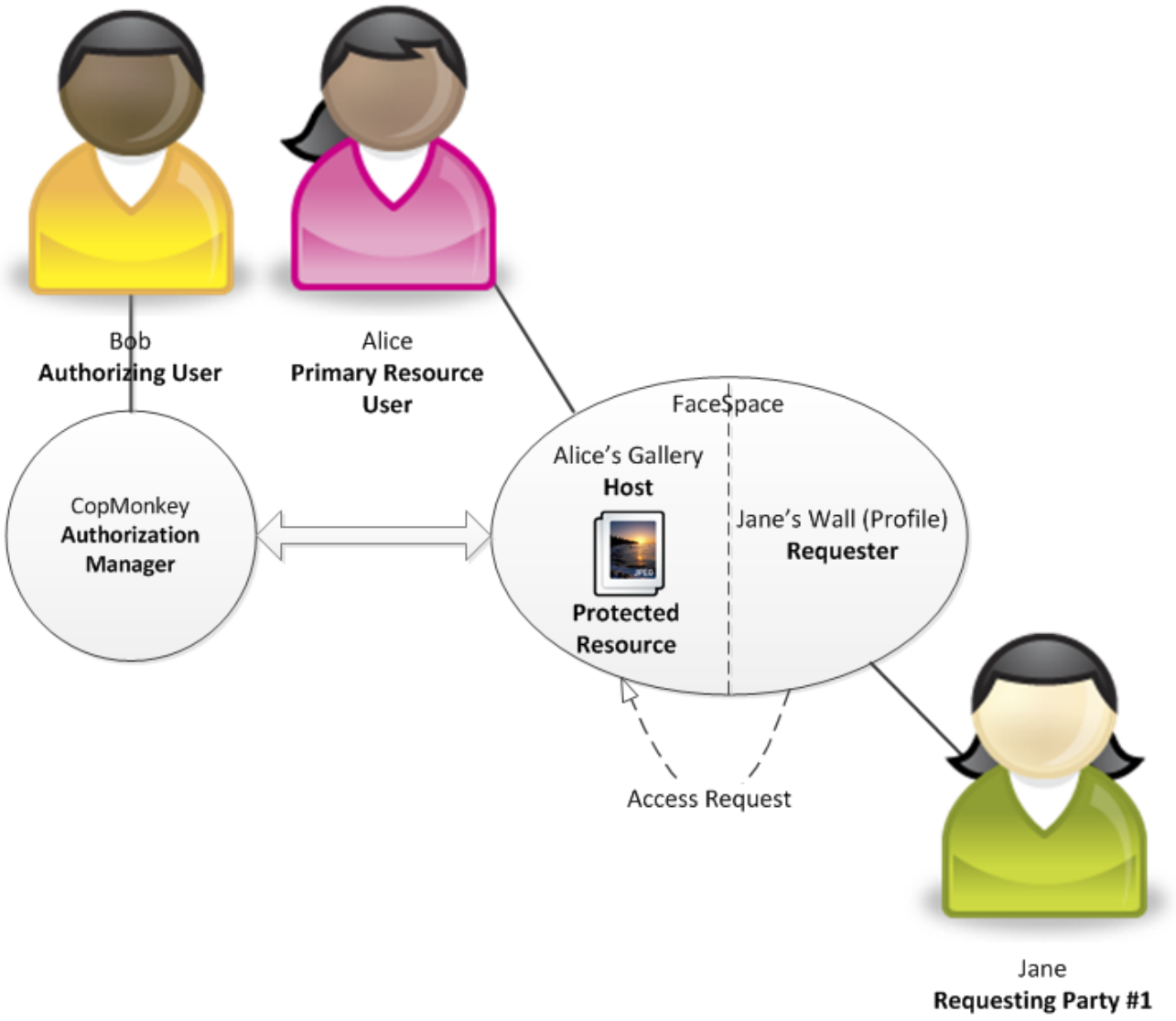
Discussion

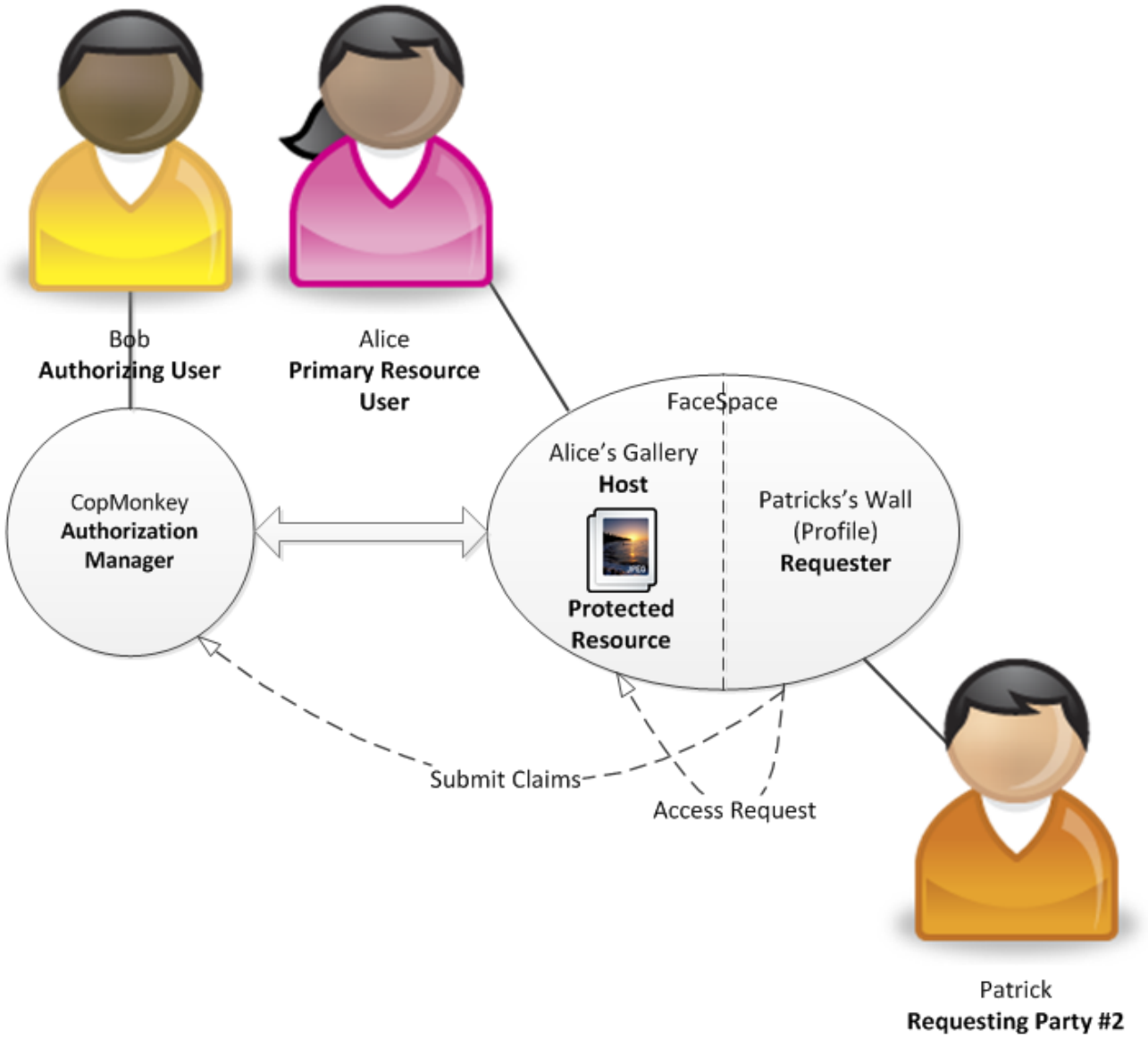
Actors in the described scenario are as following:

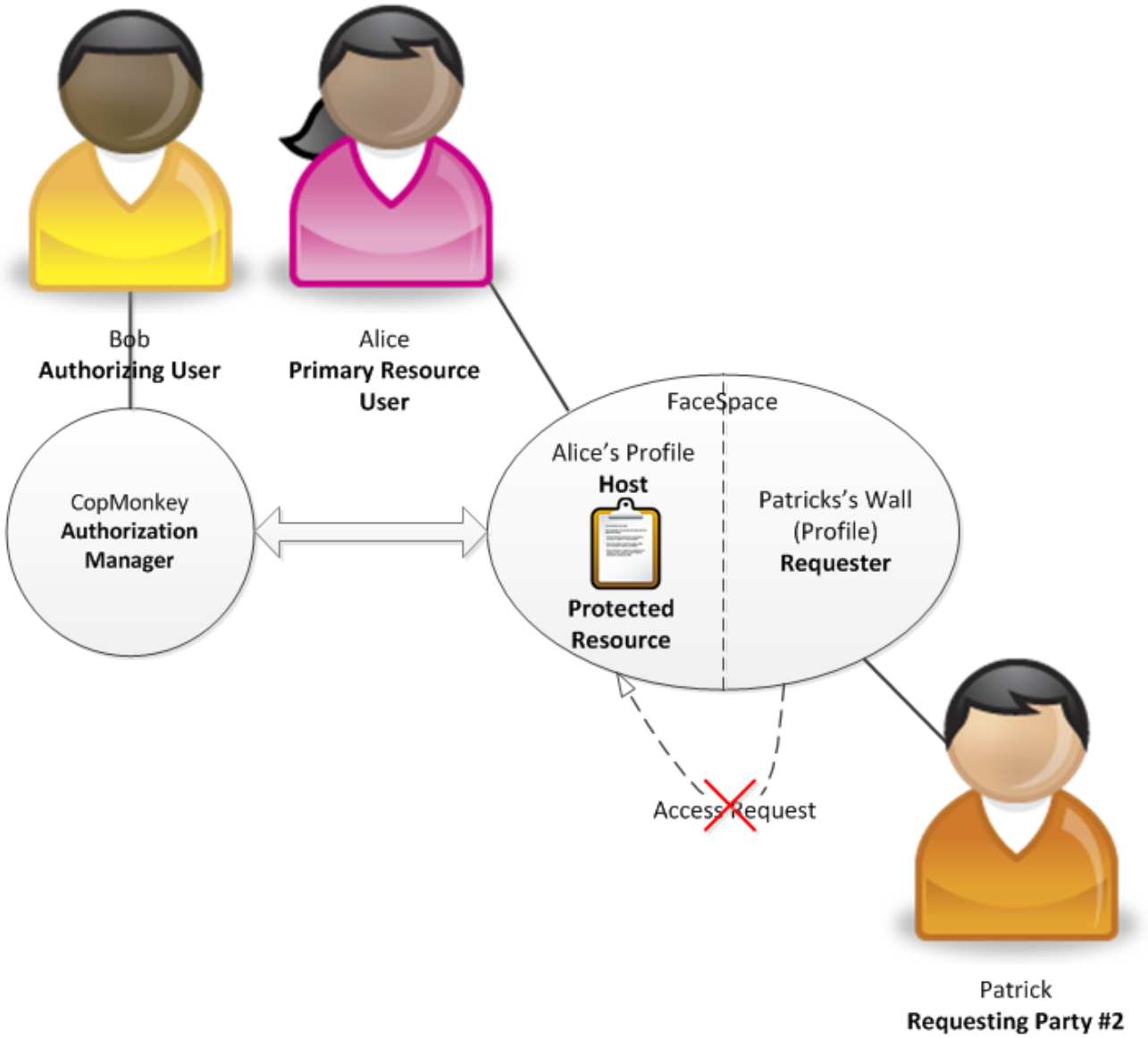
- Primary Resource User – Alice
- Authorizing User – Bob
- Protected Resource #1 – Photo
- Protected Resource #2 - Personal Information
- Host - FaceSpace
- Requester – FaceSpace
- Requesting Party #1 – Jane
- Requesting Party #2 - Patrick
- Authorization Manager – CopMonkey

Distinctive aspects:

- The typical UMA Authorizing User is split into two roles: Primary Resource User and Authorizing User (Custodian)
- UMA serves the purpose of Mandatory Access Control (MAC) with regards to Discretionary Access Control (DAC). MAC policies are defined by Bob. They are unconditionally enforced and cannot be overridden by sharing options chosen by Alice.
- The same Web application acts as a Host and a Requester, externalizing part of its access control functionality to AM.
- Claims provided by the Requester must be certified by an authoritative body (e.g. Jane needs to provide a certified claim that she is a friend of Alice – such claim is signed by FaceSpace)


Bob
Authorizing User
Alice
Primary Resource User
CopMonkey
Authorization Manager
FaceSpace
Alice's Gallery
Host
Protected Resource
Jane's Wall (Profile)
Requester
Access Request
Jane
Requesting Party #1


Bob
Authorizing User
Alice
Primary Resource User
FaceSpace
Alice's Gallery
Host
Protected Resource
Patricks's Wall (Profile)
Requester
CopMonkey
Authorization Manager
Submit Claims
Access Request
Patrick
Requesting Party #2



The following scenario shows how a user can delegate (a part of) access control functionality to a different user. In this case, an owner of a resource decides that a different entity (a custodian) will be also responsible for security of their resources. A user is concerned with producing and submitting content on the Web and may define sharing options for such content (e.g. Alice can upload a picture and define who sees that picture). However, it is the custodian that is responsible for ensuring that such content is well protected by defining mandatory access control policies. Such MAC rules cannot be overridden by rules defined by the primary resource user (e.g. Bob may define a rule that Alice's photos can be shared with her friends only which may restrict Alice's sharing options). It is then up to the custodian what access control rules are applied effectively to resources. An Authorization Manager in such setting can be viewed as an access control module externalized from a Web application that is simply under control of a different entity. Such Authorization Manager may serve the purpose of Mandatory Access Control.

A custodian can be fully responsible for defining access control policies and may be fully separated from an owner of resources. In the described scenario, Bob could be the only entity that defines access control rules for Alice's resources and Alice would only be concerned with producing and submitting these resources to FaceSpace. In such case no direct interactions are needed between the primary resource user and an authorizing user. A primary resource user may not have any knowledge about the security that is applied to a resource. As such, he or she can focus on the main tasks related to producing a resource (e.g. writing a document, submitting a photo) and can leave applying security to those who have greater knowledge and experience in defining security rules.

In the scenario, a particular Host could only accept to establish its trust relationship with a whitelisted AM. Such AM would be able to certify that a particular Authorizing User is an adult and a legal guardian of the Primary Resource User. Bob needs to get involved in the registration process to establish a trust-relationship between FaceSpace and CopMonkey. Another option for Bob, for example, would be to get an email with the instructions concerning introducing FaceSpace to AM and to perform this introduction later. Before this happens (i.e. resources submitted by Alice are protected by an adult),
Alice can share resources by herself but FileSpace will not accept any liability for potential injuries that Alice may suffer from.