Guidewire

Access Control Lists

6.0

7 October 2009

Lesson Objectives

By the end of this lesson, you should be able to:

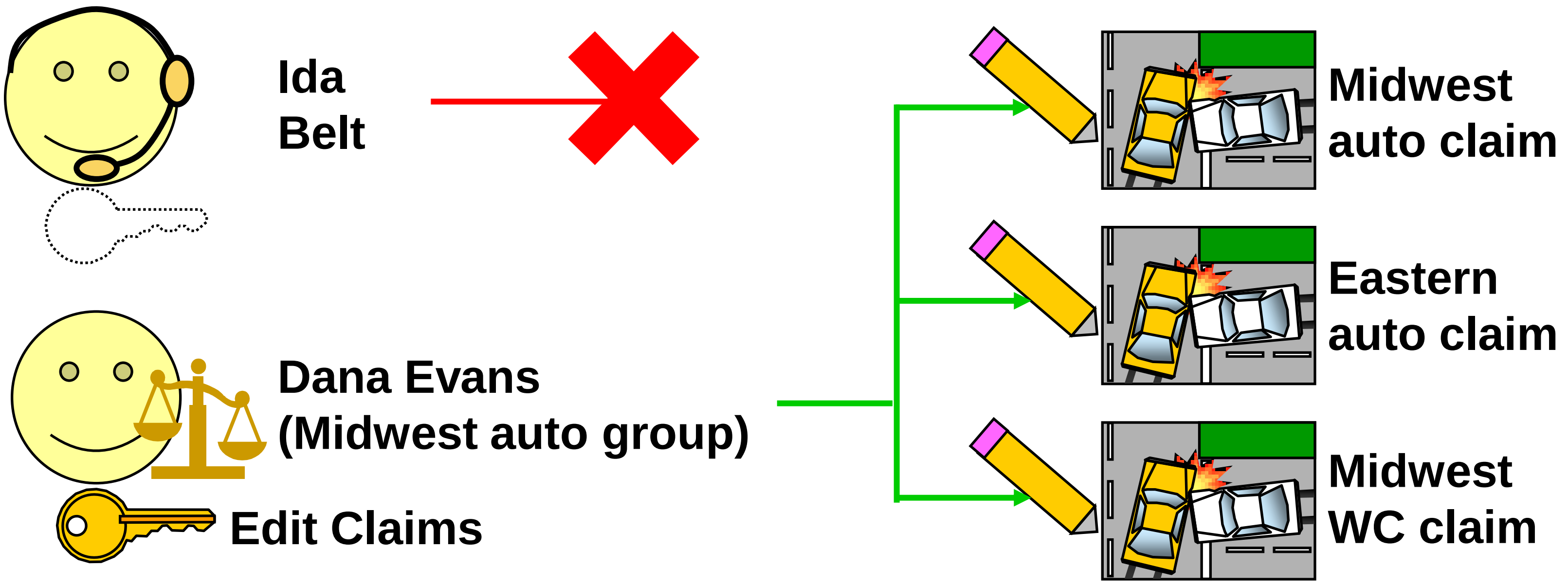
- Describe the business needs for access control
- Describe the functionality of Access Control Lists (ACLs)
- Describe the configuration options for the security profiles used to create access control lists

This lesson uses the notes section for additional explanation and information.
To view the notes in PowerPoint, choose View→Normal or View→Notes Page.
If you choose to print the notes for the lesson, be sure to select “Print hidden slides.”

Lesson Outline

- The Business Needs for Access Control
- Access Control Lists (ACLs)
- Security Profile Configuration Options

Permissions Provide "All or None" Access



Ida
Belt

Dana Evans
(Midwest auto group)

Edit Claims

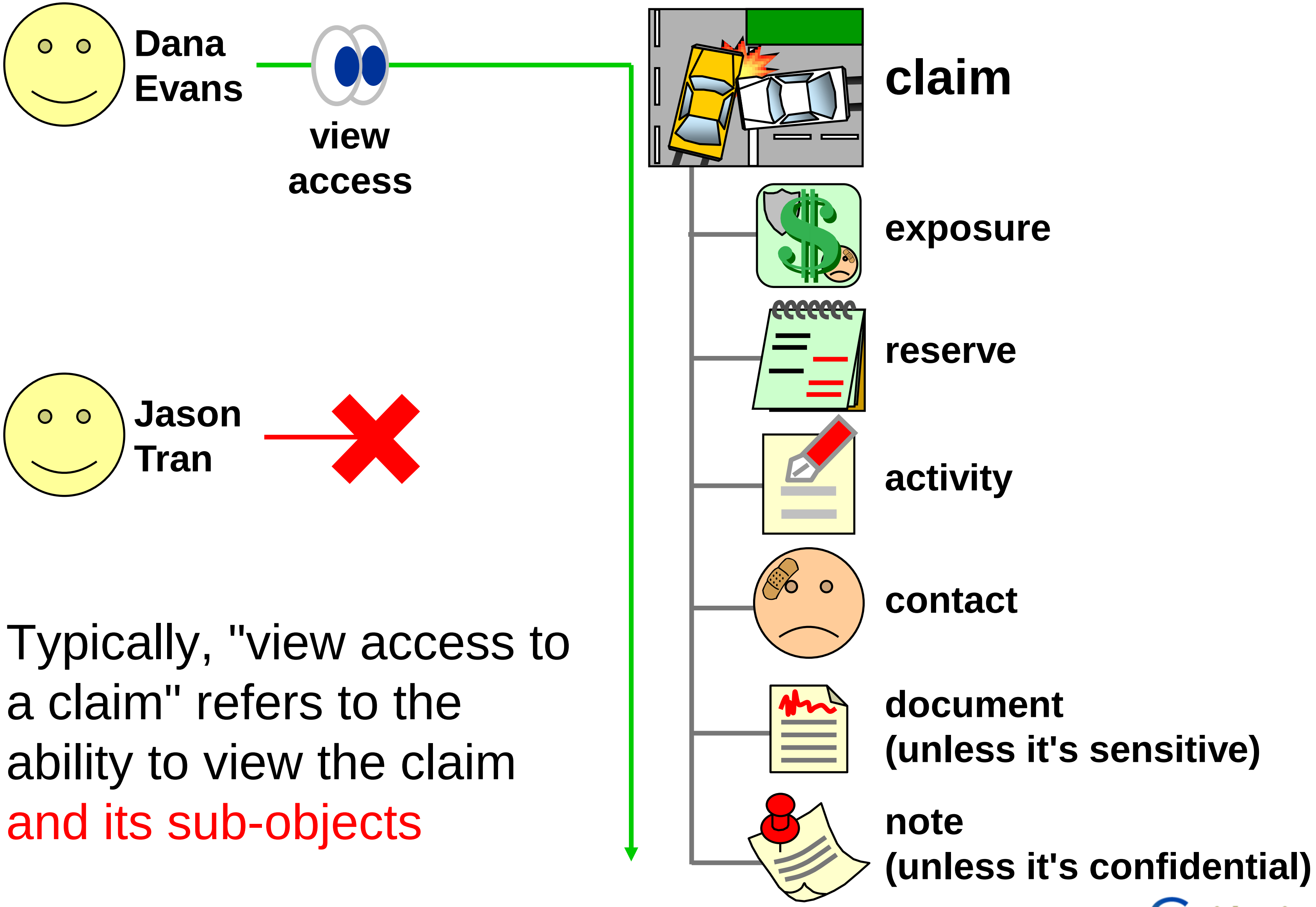
Midwest
auto claim

Eastern
auto claim

Midwest
WC claim

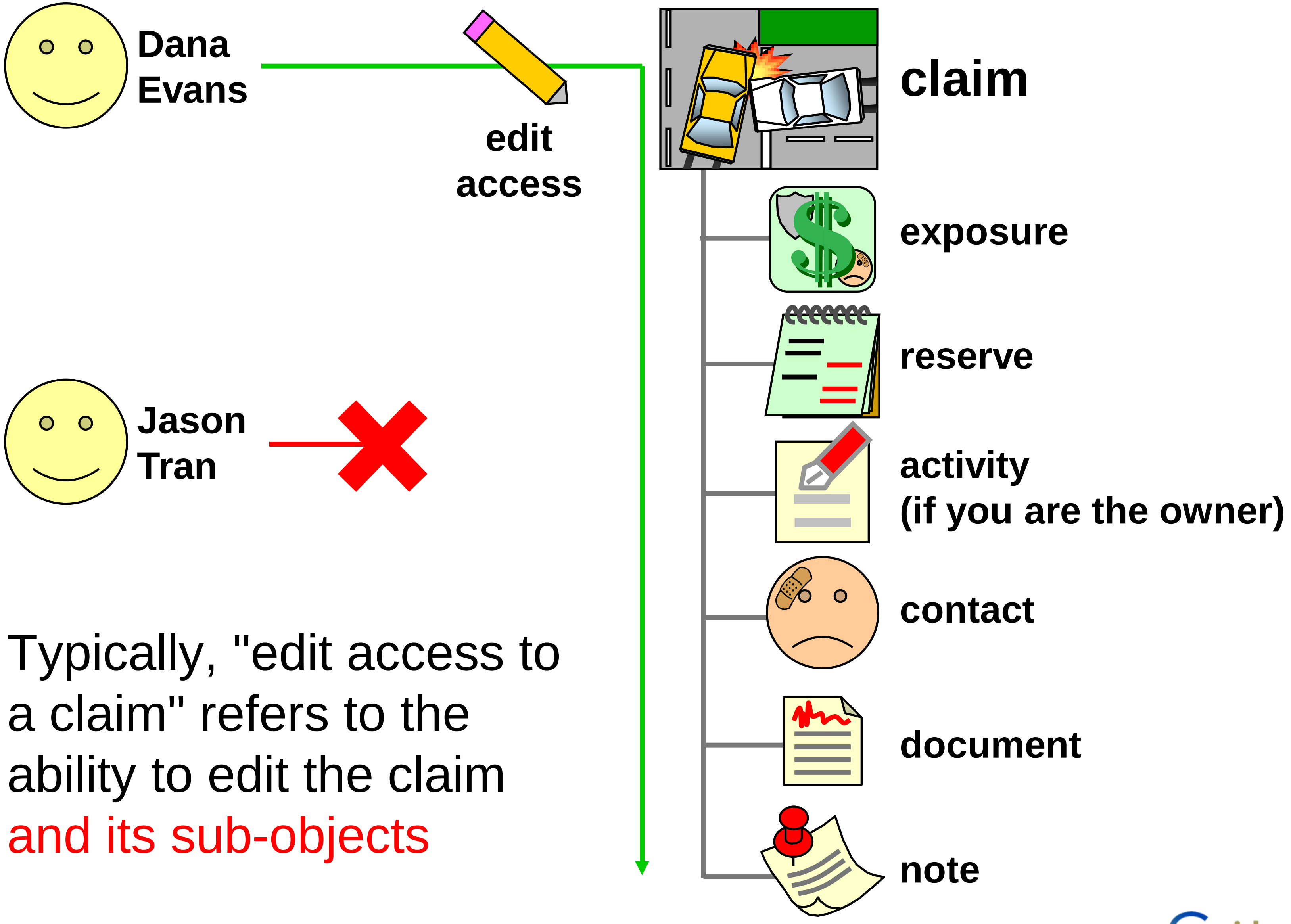
- By themselves, permissions give a user access to either:
  - All of the objects of a given entity class, or
  - None of the objects of a given entity class
- Most carriers have business needs that cannot be achieved using an "all or nothing" approach

What Is "View Claim Access"?



- Typically, "view access to a claim" refers to the ability to view the claim and its sub-objects

What Is "Edit Claim Access"?



Dana Evans

edit access

Jason Tran

claim

exposure

reserve

activity
(if you are the owner)

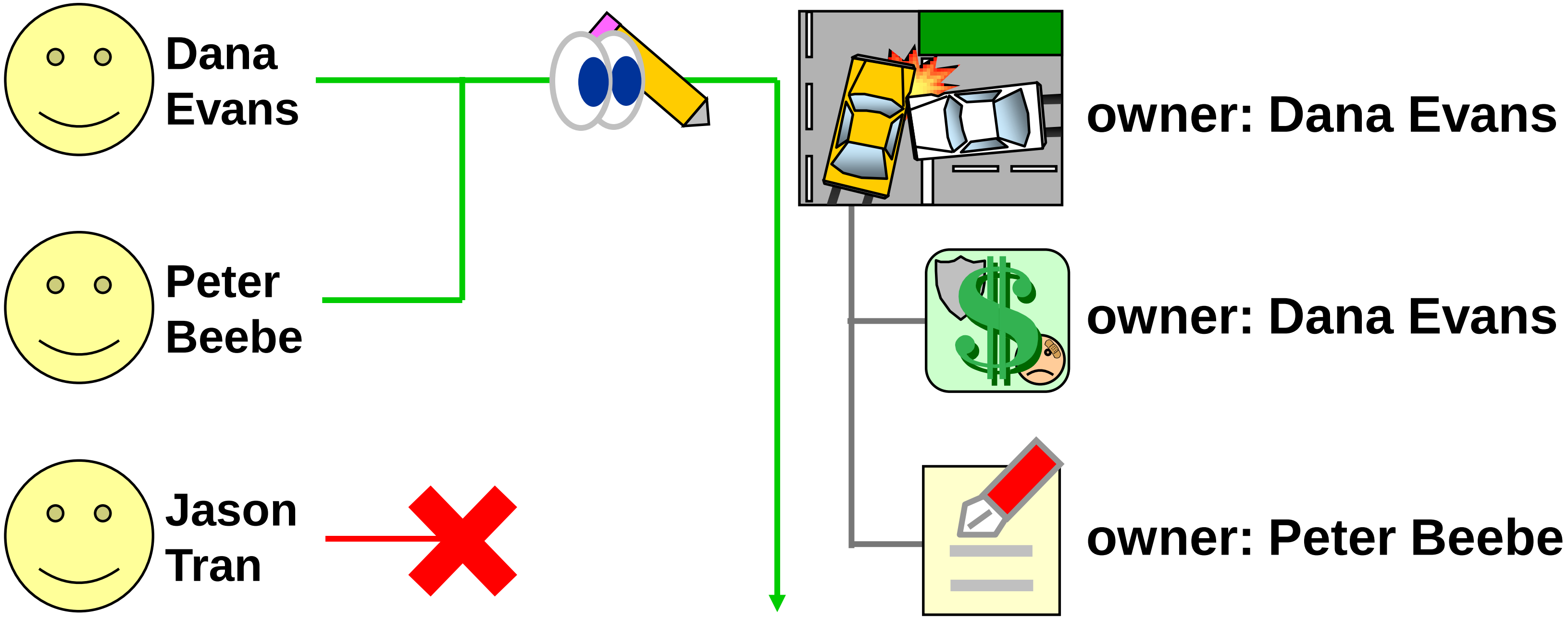
contact

document

note

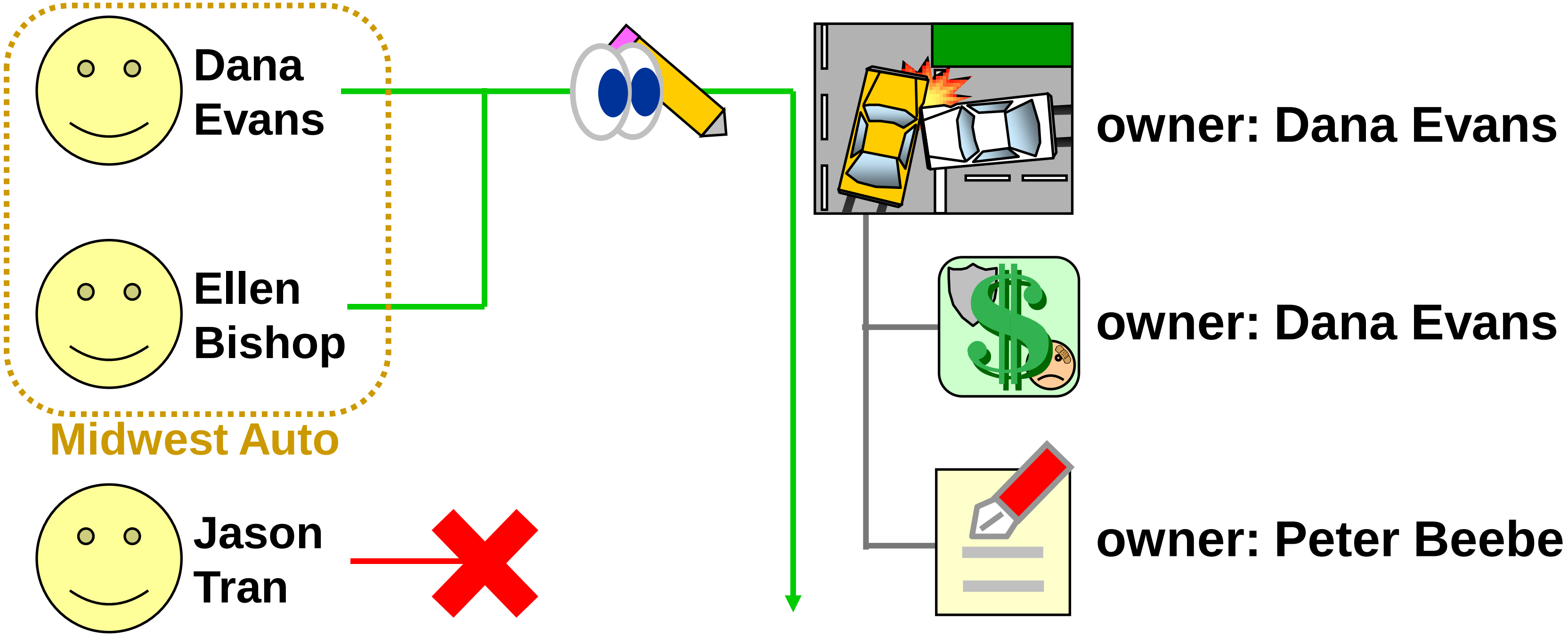
- Typically, "edit access to a claim" refers to the ability to edit the claim and its sub-objects

Business Need 1: Access to Object Owners



- In some cases, access to a given claim and all of its sub-objects should be granted to...
  - The owner of the claim itself, and possibly
  - The owners of any exposure on the claim, and possibly
  - The owners of any activities on the claim

Business Need 2: Access to People in Owner's Group



Dana Evans

Ellen Bishop

Midwest Auto

Jason Tran

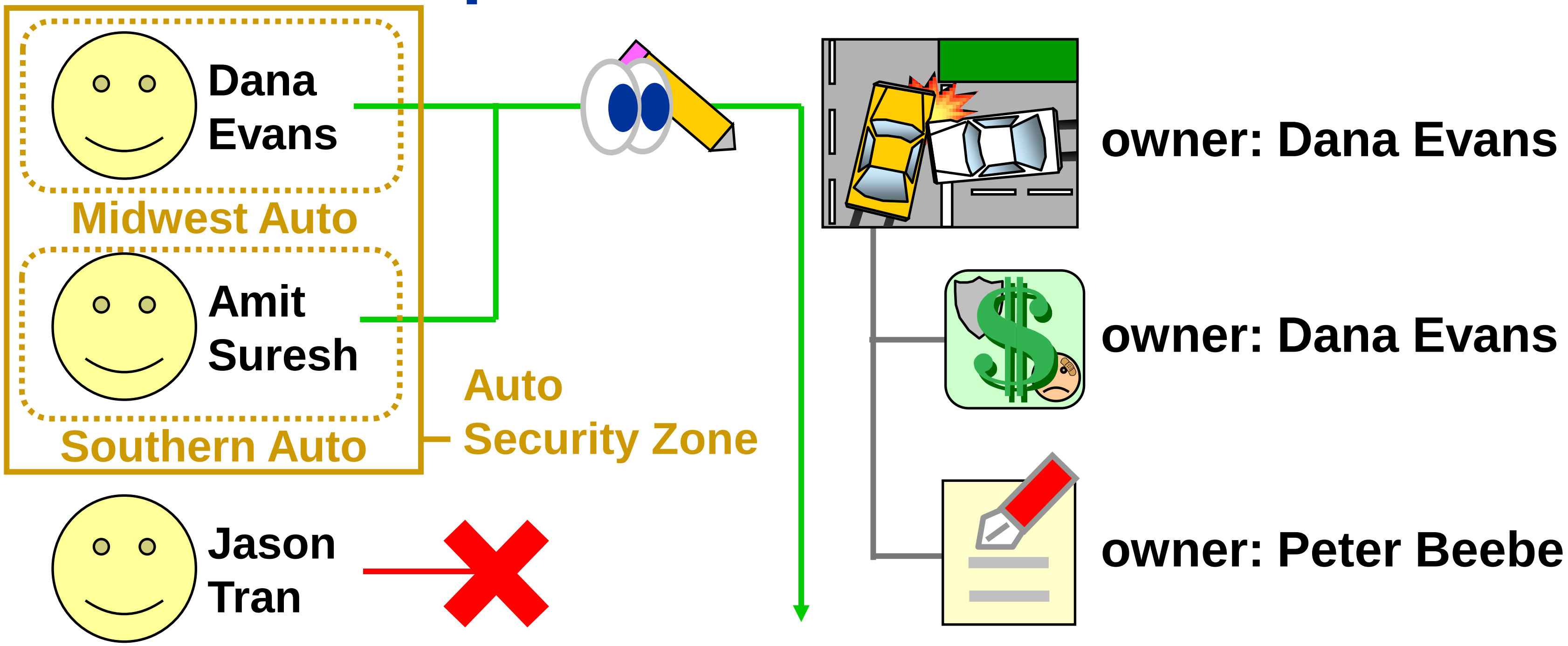
owner: Dana Evans

owner: Dana Evans

owner: Peter Beebe

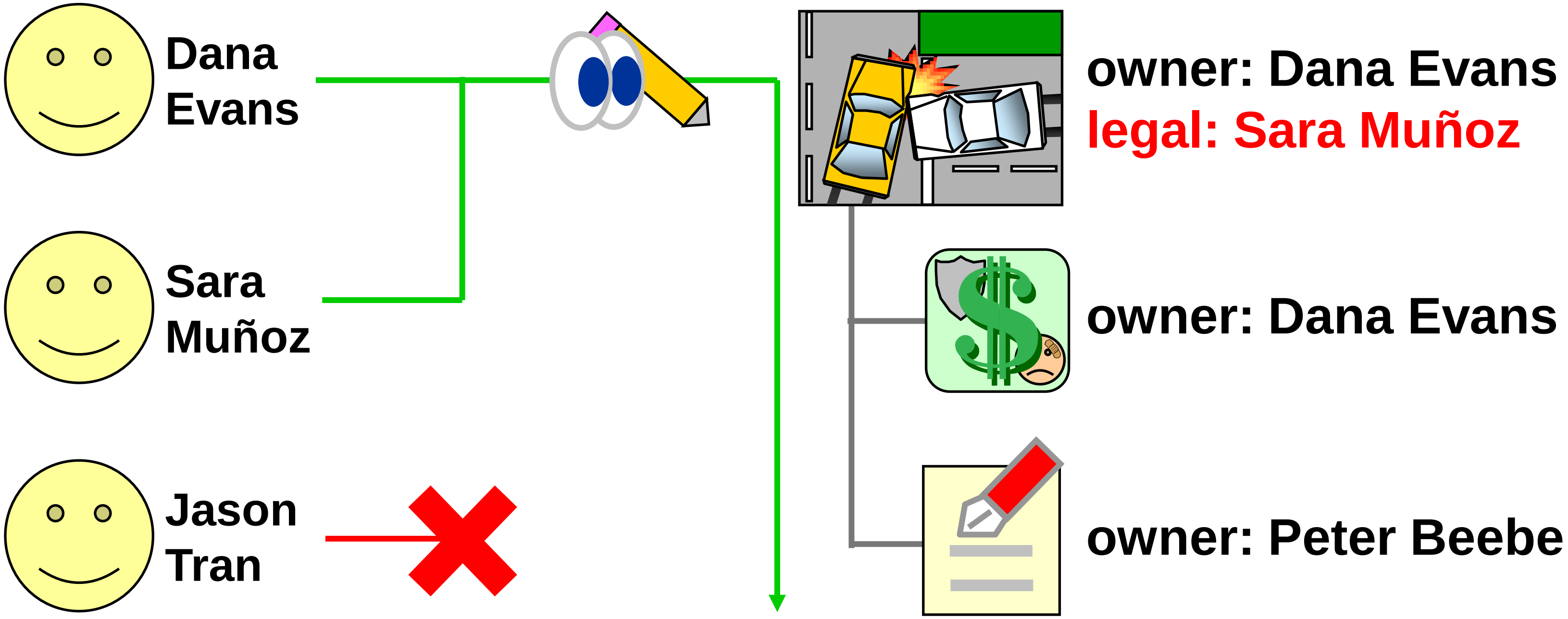
- In some cases, access to a given claim and all of its sub-objects should be granted to...
  - The users who are in the same group as the claim owner (or possibly in the same group as one of the exposure or activity owners)

Business Need 3: Access to People in Related Groups



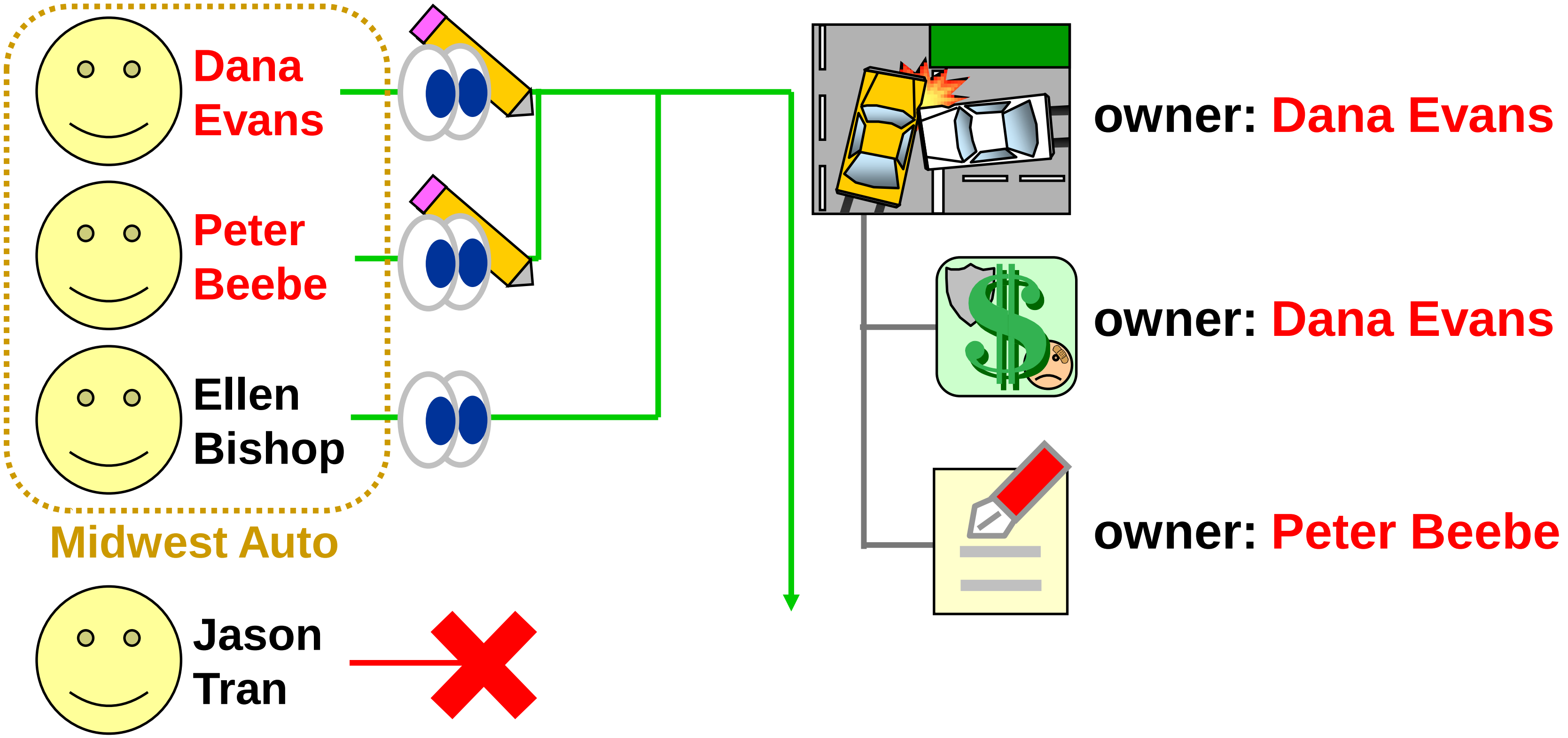
- In some cases, access to a given claim and all of its sub-objects should be granted to...
  - The users who are in a group which has a business relationship to the group to which the claim is assigned

Business Need 4: Access to Users with Claim Roles



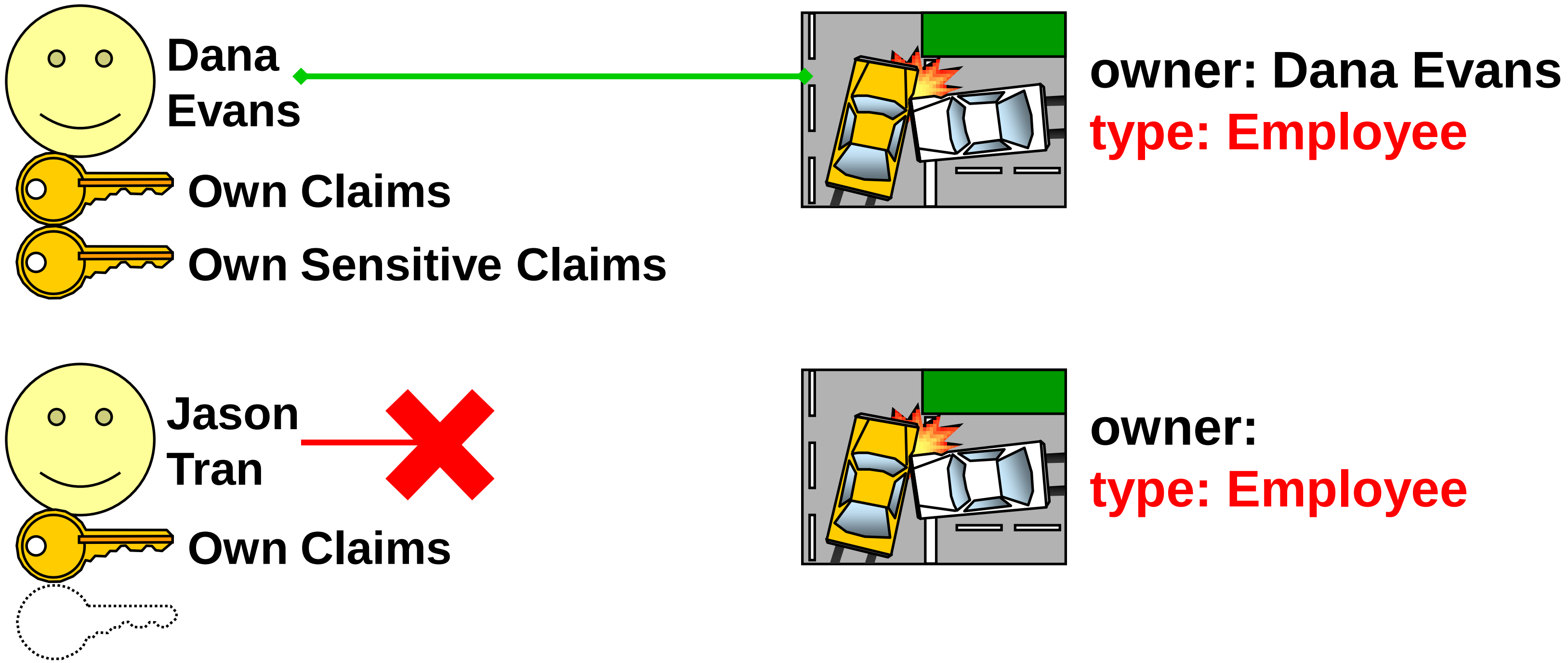
- In some cases, access to a given claim and all of its sub-objects should be granted to...
  - Any user who has a claim user role on the claim (such as legal, recovery specialist, or medical case manager)

Business Need 5: View-Only Access



- In some cases, view and edit access to a given claim and all of its sub-objects should be granted to a narrow set of users while view only access is granted to a wider set of users

Business Need 6: Claim Ownership



Dana Evans

Own Claims

Own Sensitive Claims

owner: Dana Evans

type: Employee

Jason Tran

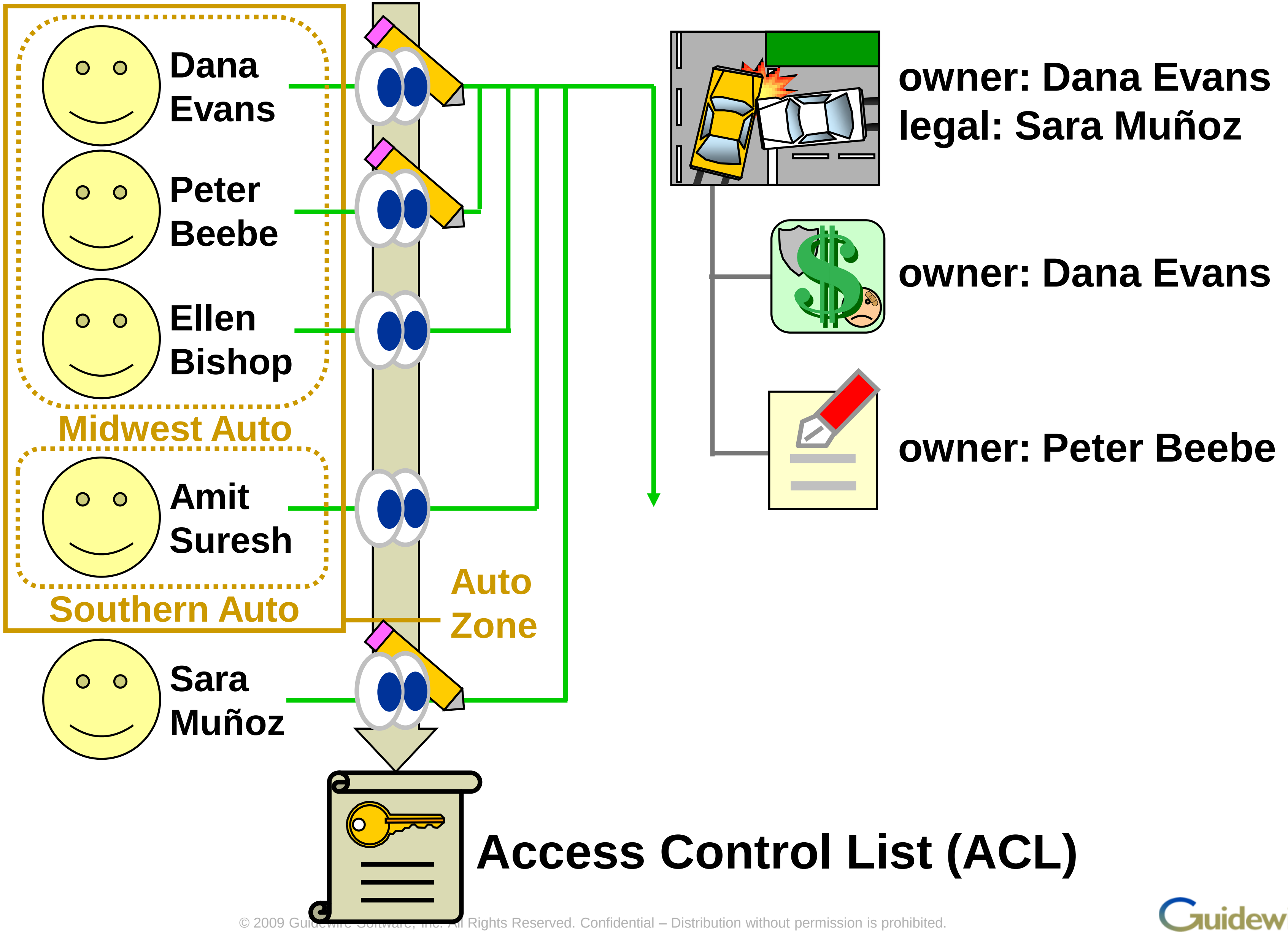
Own Claims

owner:

type: Employee

- In some cases, ownership of a given claim should be granted to...
  - Users who have the permission to own that type of claim (in addition to the basic "own claim" permission)

Meeting These Business Needs



Dana Evans

Peter Beebe

Ellen Bishop

Midwest Auto

Amit Suresh

Southern Auto

Auto Zone

Sara Muñoz

owner: Dana Evans
legal: Sara Muñoz

owner: Dana Evans

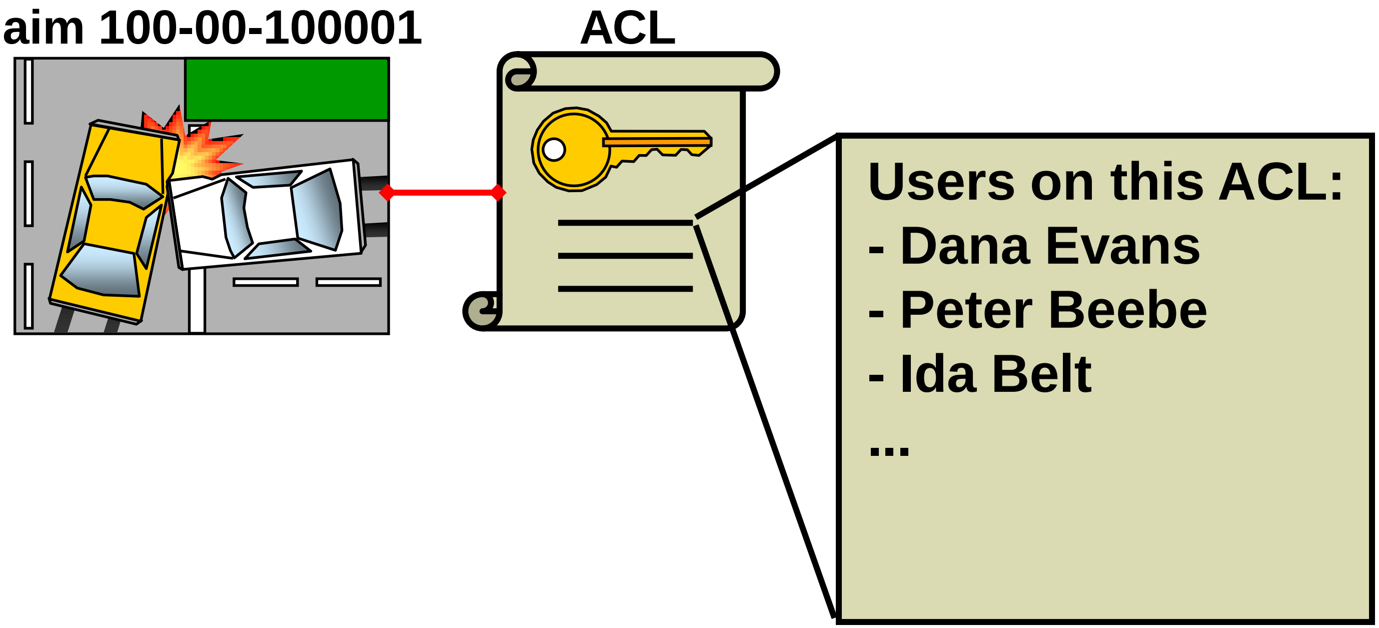
owner: Peter Beebe

Access Control List (ACL)

Lesson Outline

- The Business Needs for Access Control
- Access Control Lists (ACLs)
- Security Profile Configuration Options

Access Control Lists (ACLs)



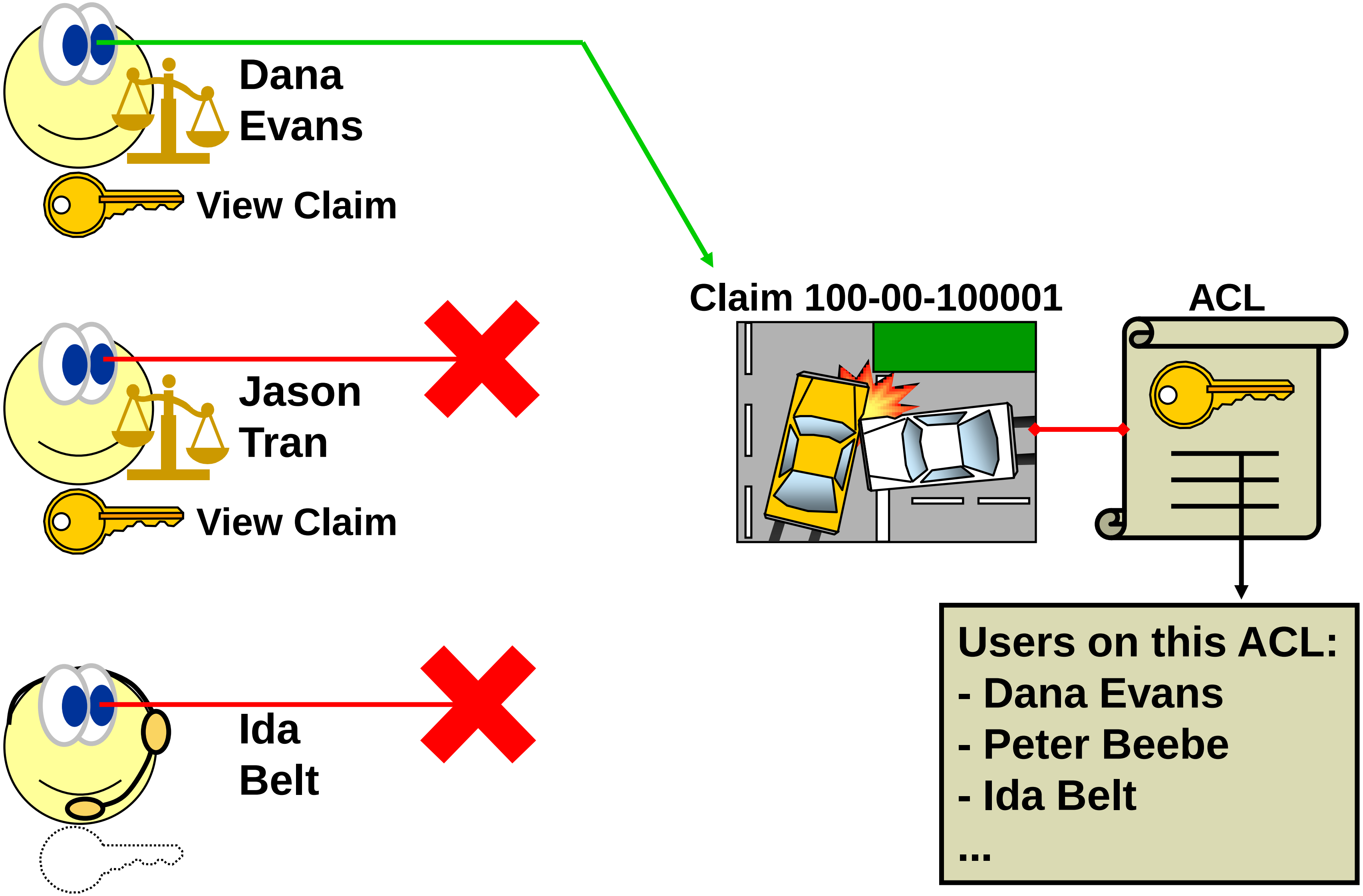
Claim 100-00-100001

ACL

Users on this ACL:
- Dana Evans
- Peter Beebe
- Ida Belt
...

- An access control list (ACL) is a list associated to a claim that identifies the users who can access the claim and its sub-objects
  - ACLs ensure that a given user can view or edit only the objects which he or she has a business need to view or edit

Permissions and ACLs



Dana Evans

View Claim

Jason Tran

View Claim

Ida Belt

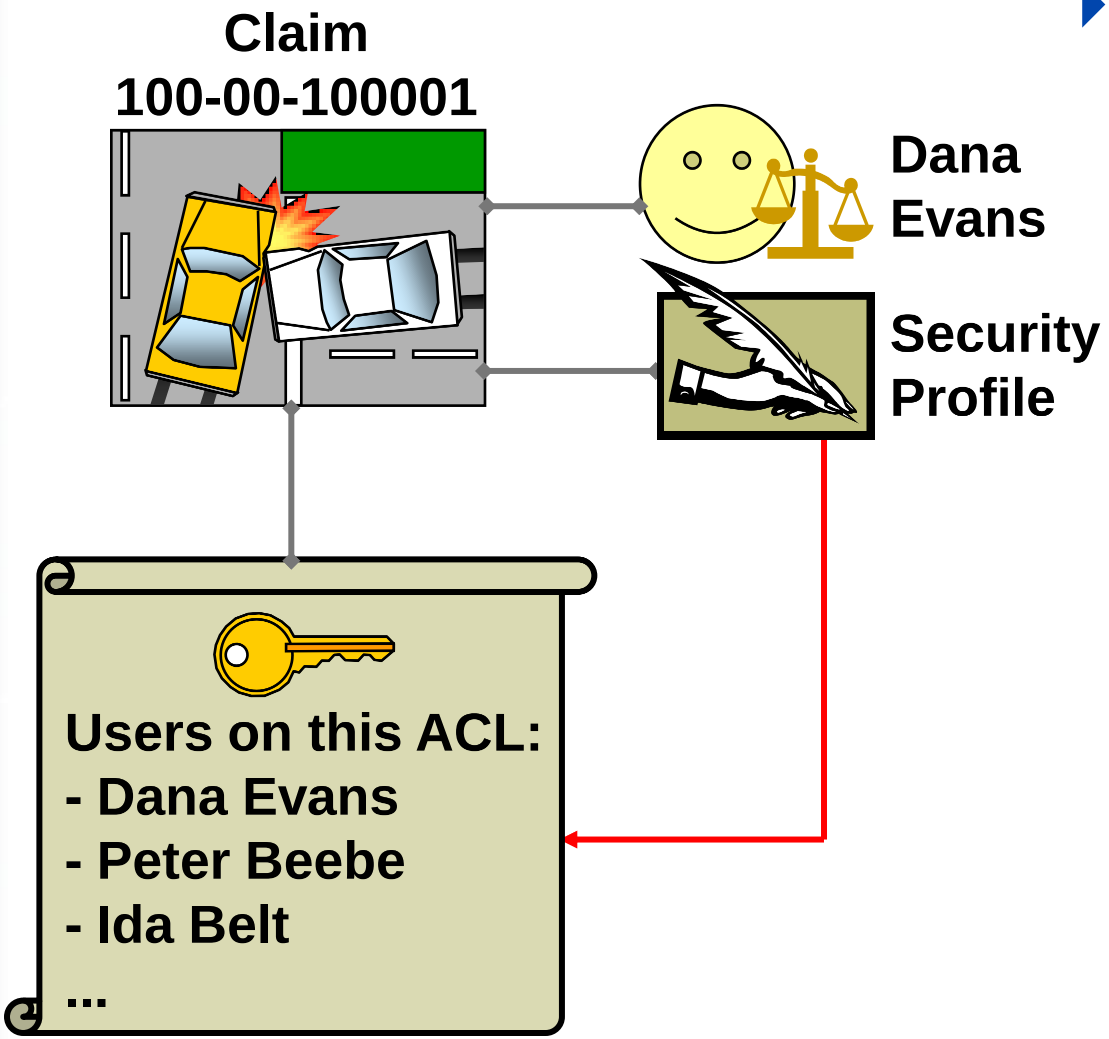
Claim 100-00-100001

ACL

Users on this ACL:
- Dana Evans
- Peter Beebe
- Ida Belt

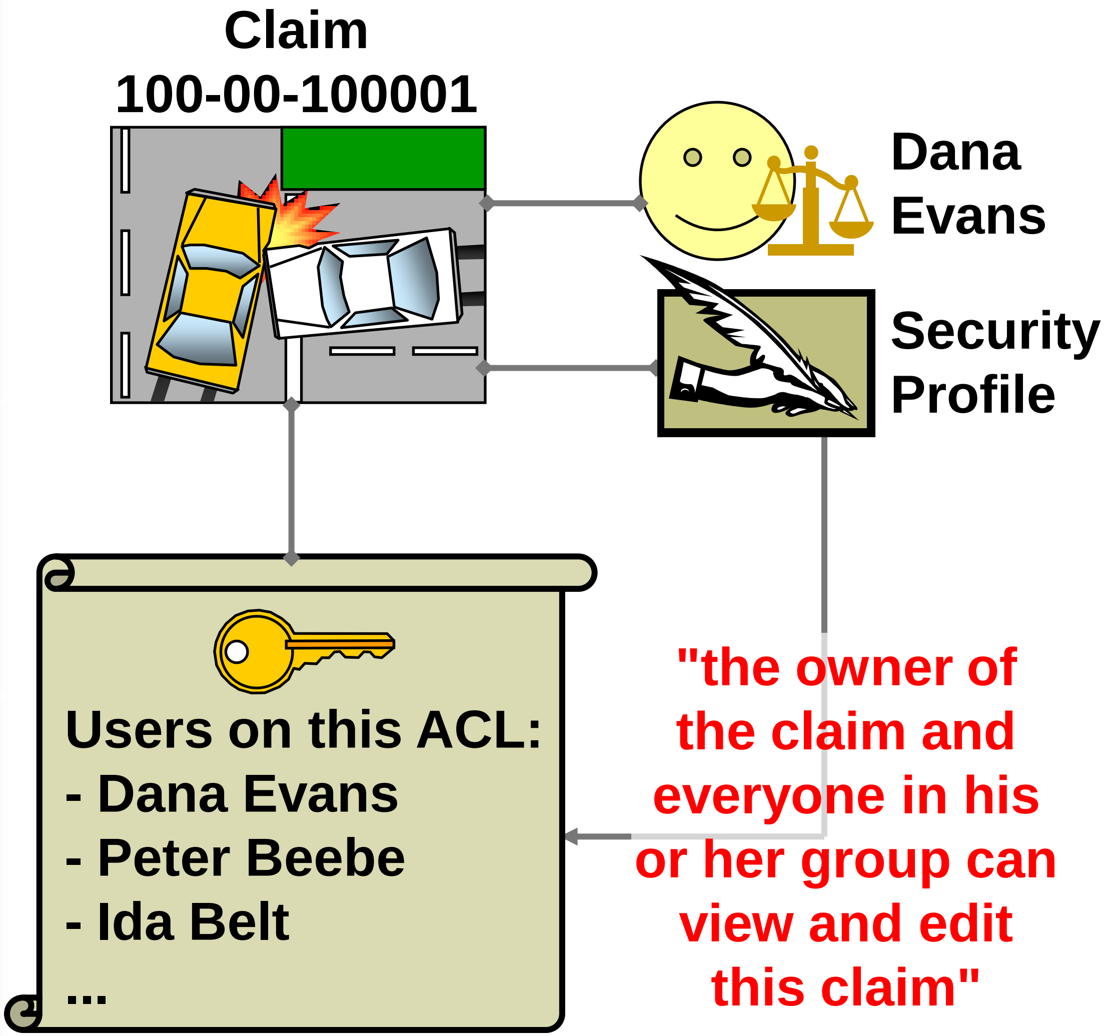
...

ACLs Are Created Using Security Profiles



- ClaimCenter automatically creates an access control list for every claim using a security profile
  - A security profile is a collection of criteria
  - Every user which meets the criteria for that claim gets on the ACL for that claim

Security Profile Criteria

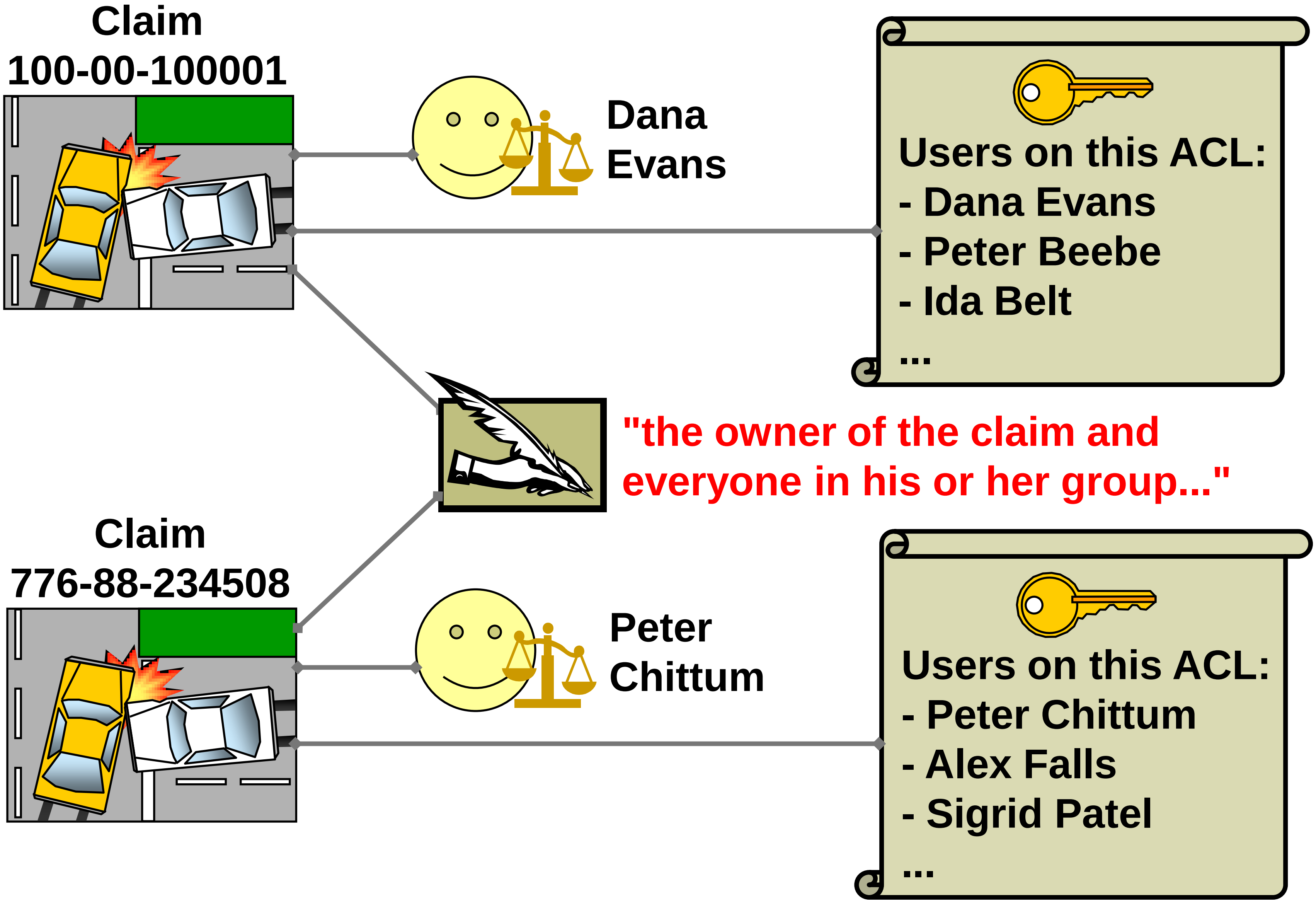


Users on this ACL:
- Dana Evans
- Peter Beebe
- Ida Belt
...

"the owner of the claim and everyone in his or her group can view and edit this claim"

- The criteria in a security profile always pertains to:
  - Owning the claim (or one of its exposures or activities)
  - Being in the same group (or security zone) as an object owner
  - Having a claim user role on the claim

A Profile Can Generate Different ACLs



Claim
100-00-100001

Dana
Evans

Users on this ACL:
- Dana Evans
- Peter Beebe
- Ida Belt
...

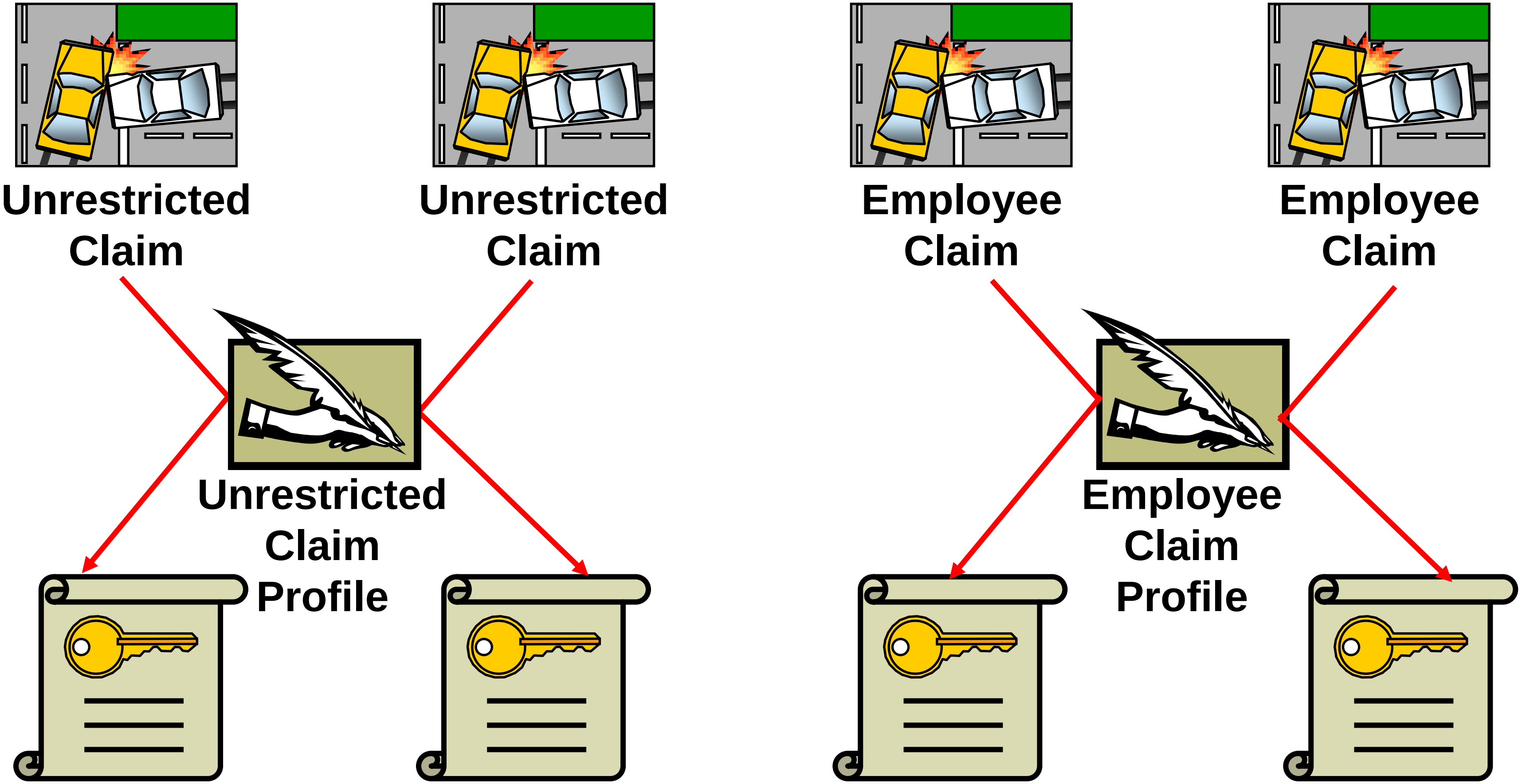
"the owner of the claim and everyone in his or her group..."

Claim
776-88-234508

Peter
Chittum

Users on this ACL:
- Peter Chittum
- Alex Falls
- Sigrid Patel
...

Multiple Security Profiles



Unrestricted Claim

Unrestricted Claim

Employee Claim

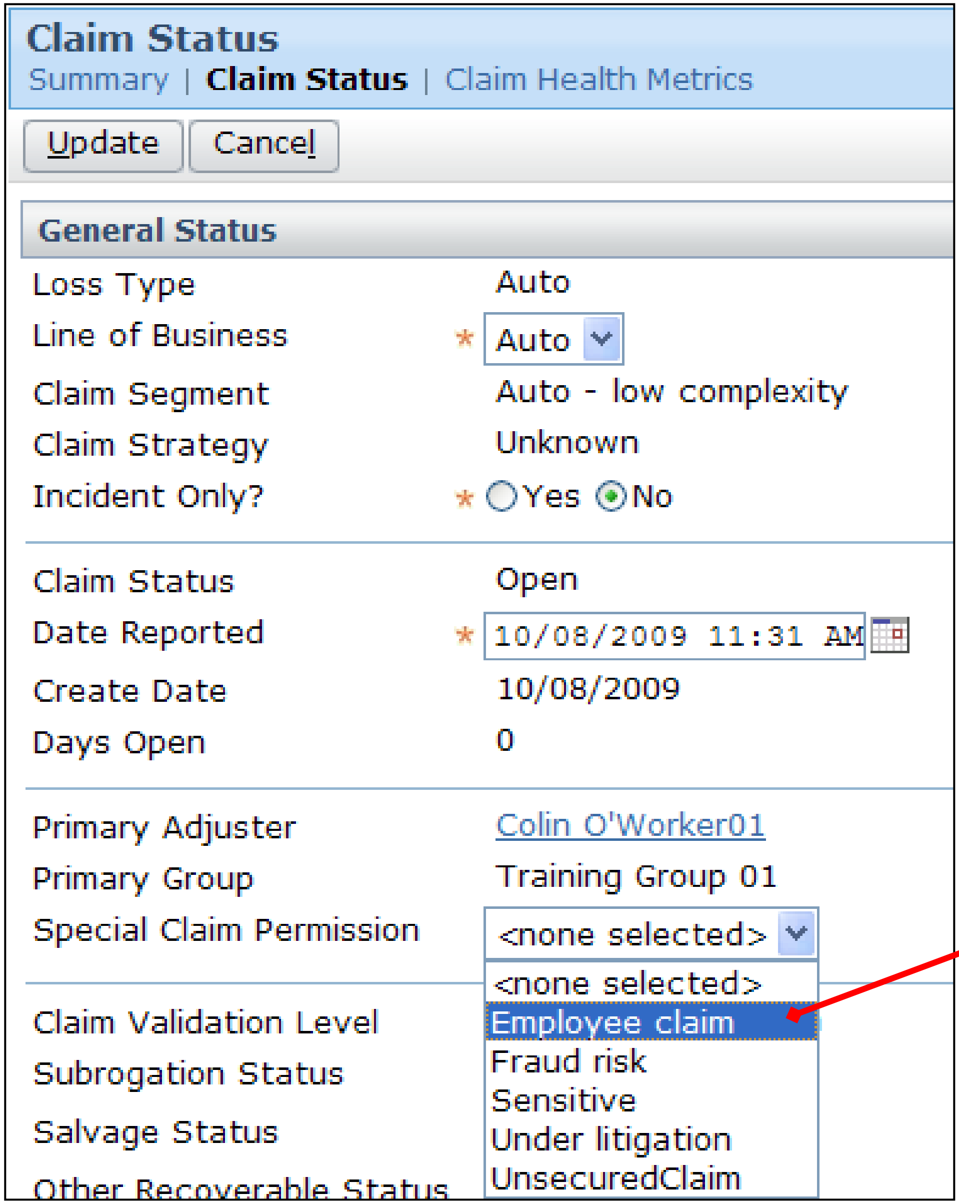
Employee Claim

Unrestricted Claim Profile

Employee Claim Profile

- A ClaimCenter implementation may use multiple security profiles
  - Each profile contains the criteria for a type of business scenario

Identifying a Claim's Security Type



Claim Status

Summary | **Claim Status** | Claim Health Metrics

General Status

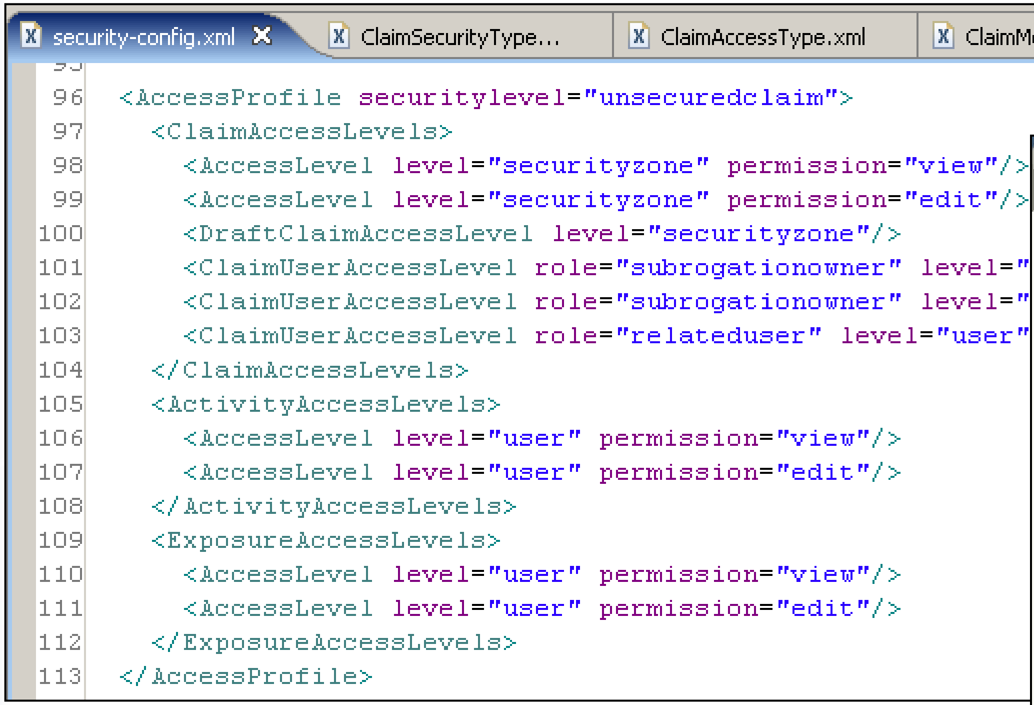
Loss Type	Auto
Line of Business	* Auto
Claim Segment	Auto - low complexity
Claim Strategy	Unknown
Incident Only?	* ○ Yes ● No
Claim Status	Open
Date Reported	* 10/08/2009 11:31 AM
Create Date	10/08/2009
Days Open	0
Primary Adjuster	Colin O'Worker01
Primary Group	Training Group 01
Special Claim Permission	<none selected>
Claim Validation Level	
Subrogation Status	
Salvage Status	
Other Recoverable Status	

Employee Claim Profile

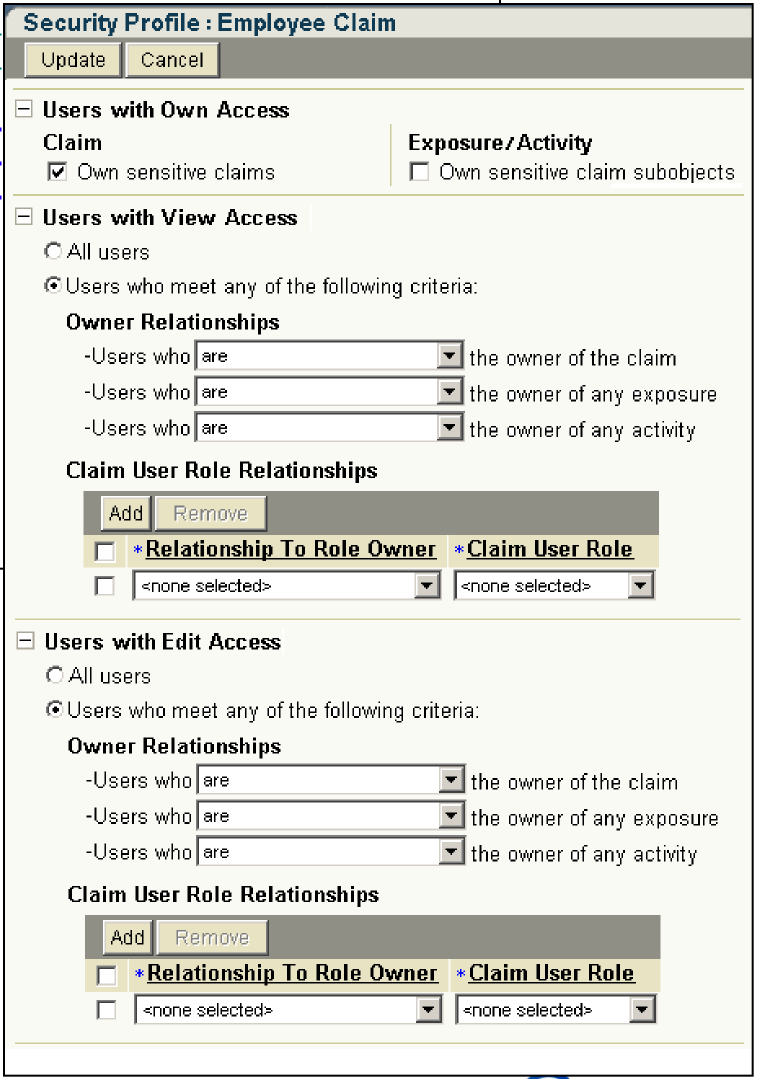
Lesson Outline

- The Business Needs for Access Control
- Access Control Lists (ACLs)
- Security Profile Configuration Options

Configuring Security Profiles



```
<AccessProfile securitylevel="unsecuredclaim">
  <ClaimAccessLevels>
    <AccessLevel level="securityzone" permission="view"/>
    <AccessLevel level="securityzone" permission="edit"/>
    <DraftClaimAccessLevel level="securityzone"/>
    <ClaimUserAccessLevel role="subrogationowner" level="
    <ClaimUserAccessLevel role="subrogationowner" level="
    <ClaimUserAccessLevel role="relateduser" level="user"
  </ClaimAccessLevels>
  <ActivityAccessLevels>
    <AccessLevel level="user" permission="view"/>
    <AccessLevel level="user" permission="edit"/>
  </ActivityAccessLevels>
  <ExposureAccessLevels>
    <AccessLevel level="user" permission="view"/>
    <AccessLevel level="user" permission="edit"/>
  </ExposureAccessLevels>
</AccessProfile>
```



Security Profile : Employee Claim

Users with Own Access

Claim: ☑ Own sensitive claims

Exposure/Activity: □ Own sensitive claim subobjects

Users with View Access

○ All users

● Users who meet any of the following criteria:

Owner Relationships

-Users who are the owner of the claim

-Users who are the owner of any exposure

-Users who are the owner of any activity

Claim User Role Relationships

□	*Relationship To Role Owner	*Claim User Role
□	<none selected>	<none selected>

Users with Edit Access

○ All users

● Users who meet any of the following criteria:

Owner Relationships

-Users who are the owner of the claim

-Users who are the owner of any exposure

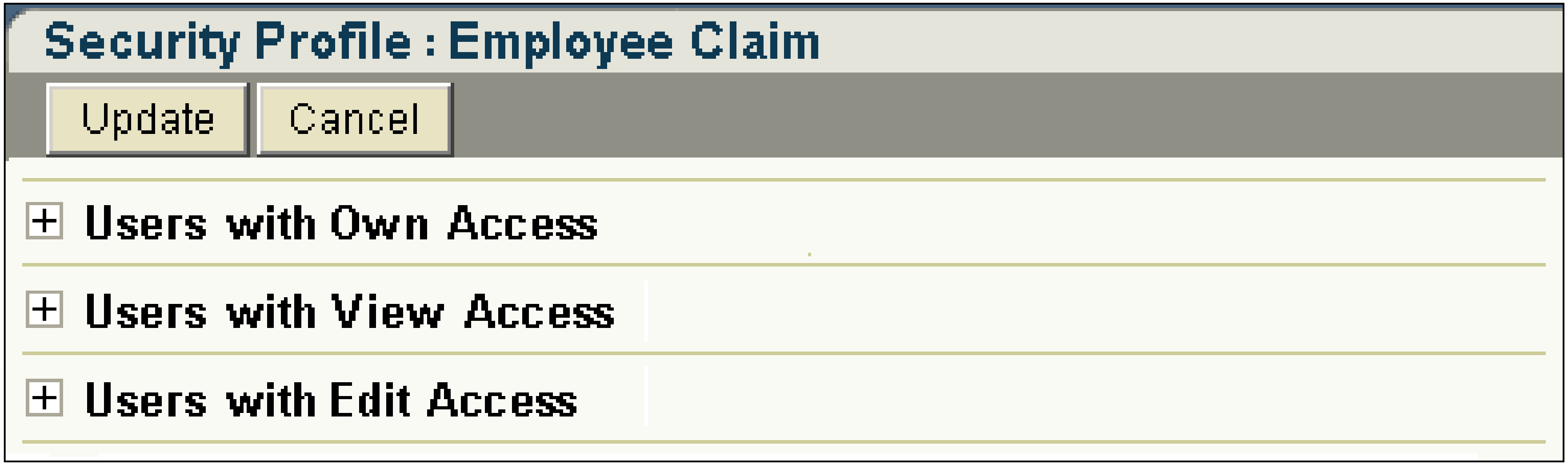
-Users who are the owner of any activity

Claim User Role Relationships

□	*Relationship To Role Owner	*Claim User Role
□	<none selected>	<none selected>

- Security profiles are configured by consultants using XML
  - The following slides use a fictional "security profile UI" to simplify the discussion of what a security profile can do

Major Portions of a Security Profile



Security Profile : Employee Claim

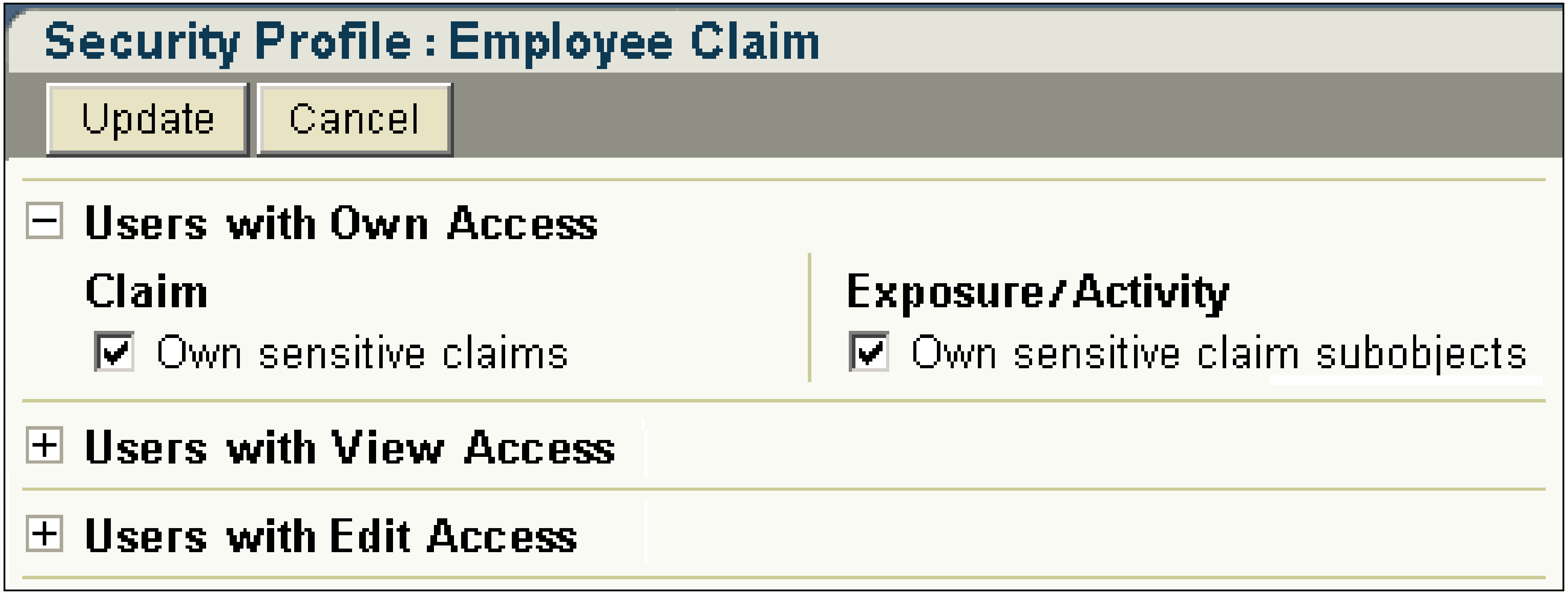
⊞ Users with Own Access

⊞ Users with View Access

⊞ Users with Edit Access

- A security profile can specify:
  - Permissions a user must have to own this type of claim (or its sub-objects)
  - Criteria users must meet to be able to view the claim
  - Criteria users must meet to be able to edit the claim

Specifying Own Access



Security Profile : Employee Claim

− Users with Own Access

Claim

☑ Own sensitive claims

Exposure/Activity

☑ Own sensitive claim subobjects

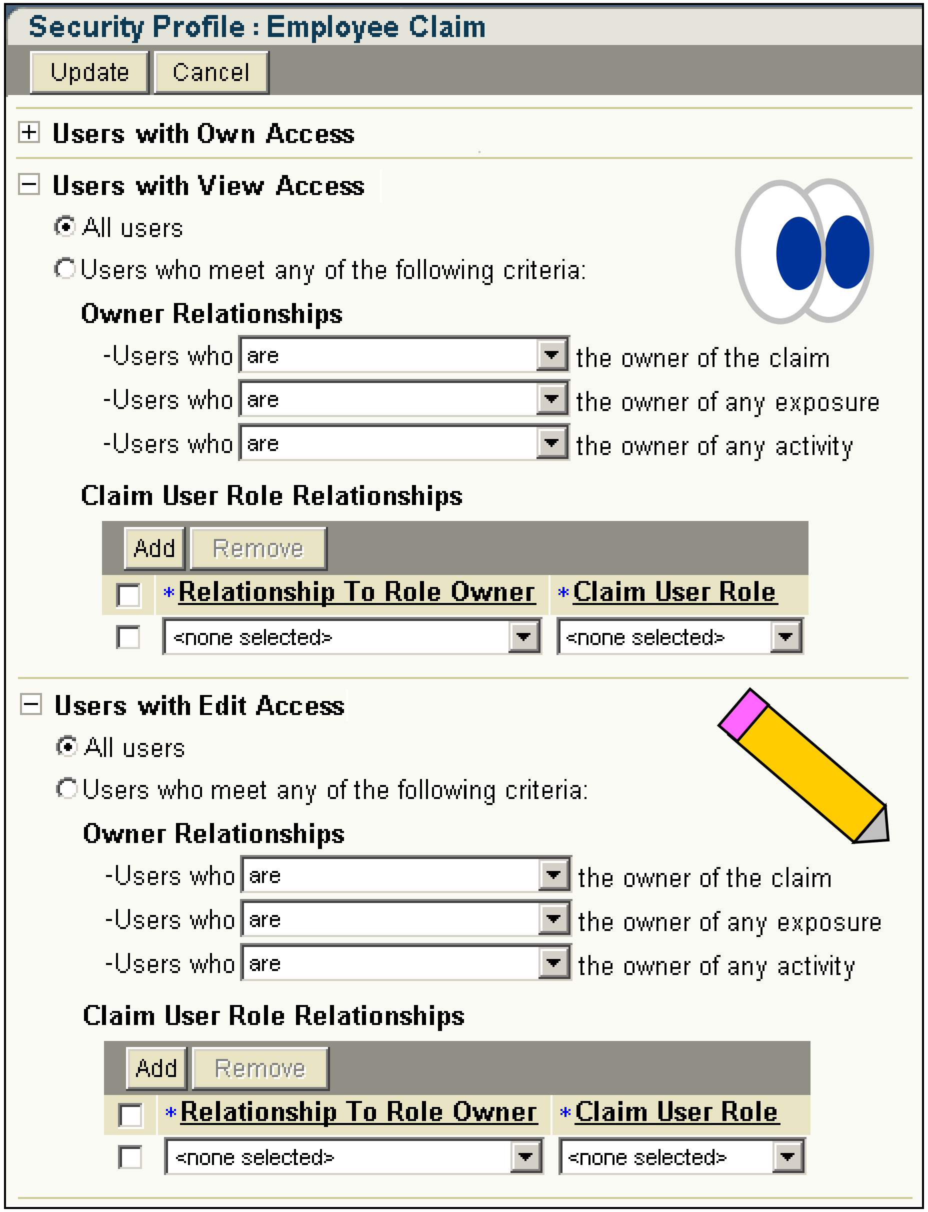
+ Users with View Access

+ Users with Edit Access

- A security profile can specify one or more permissions a user must have (in addition to "own claim", "own exposure", and/or "own activity") to own a claim of this security type

Specifying View and Edit Access

- For view and edit access, the security profile contains a set of criteria
  - Users who meet the criteria have the view and/or edit permission set



Security Profile : Employee Claim

⊞ **Users with Own Access**

⊟ **Users with View Access**

● All users

○ Users who meet any of the following criteria:

Owner Relationships

-Users who are the owner of the claim

-Users who are the owner of any exposure

-Users who are the owner of any activity

Claim User Role Relationships

□	***Relationship To Role Owner**	***Claim User Role**
□	<none selected>	<none selected>

⊟ **Users with Edit Access**

● All users

○ Users who meet any of the following criteria:

Owner Relationships

-Users who are the owner of the claim

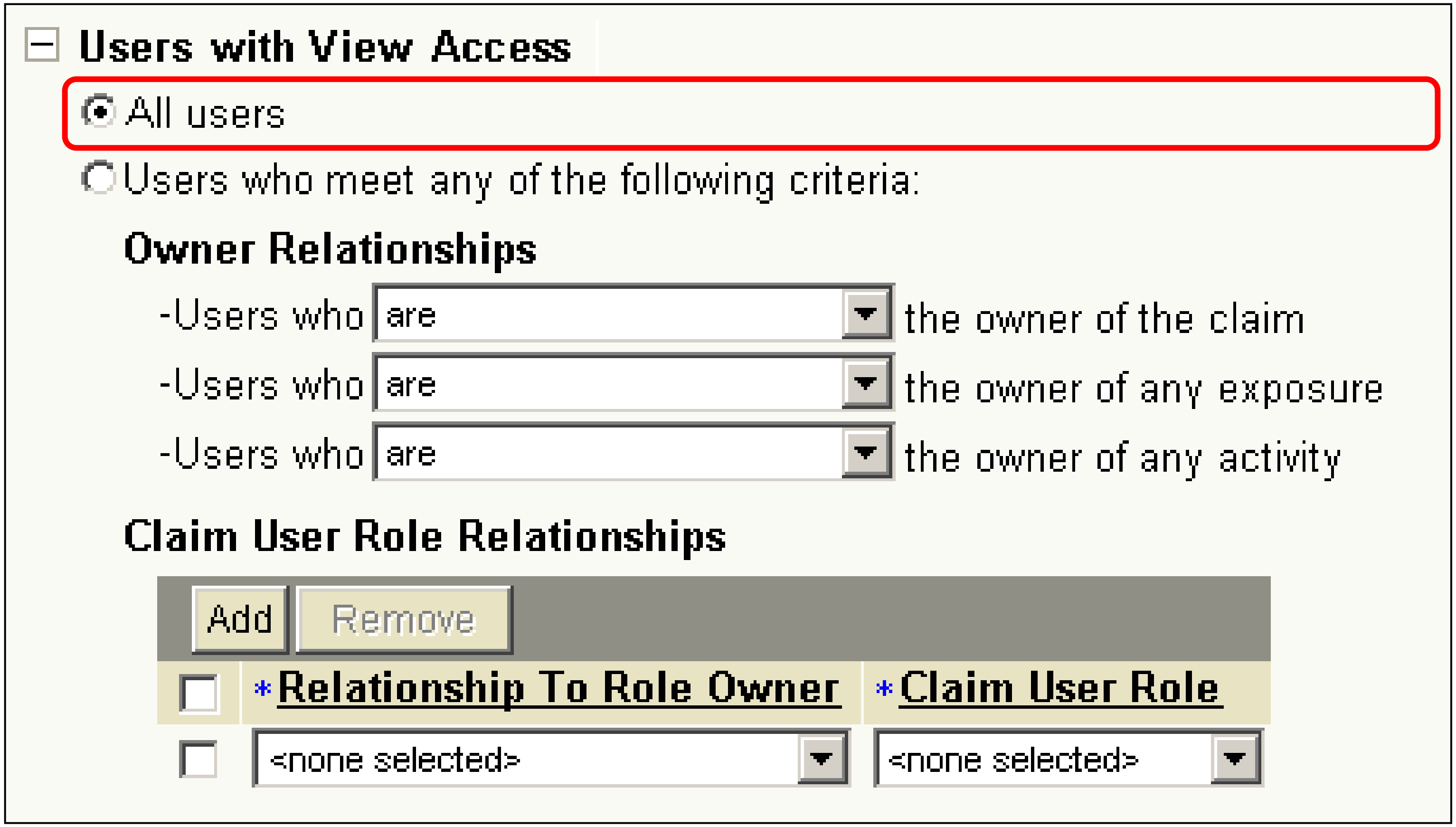
-Users who are the owner of any exposure

-Users who are the owner of any activity

Claim User Role Relationships

□	***Relationship To Role Owner**	***Claim User Role**
□	<none selected>	<none selected>

View Access: All Users



⊟ **Users with View Access**

● All users

○ Users who meet any of the following criteria:

Owner Relationships

-Users who are ▾ the owner of the claim

-Users who are ▾ the owner of any exposure

-Users who are ▾ the owner of any activity

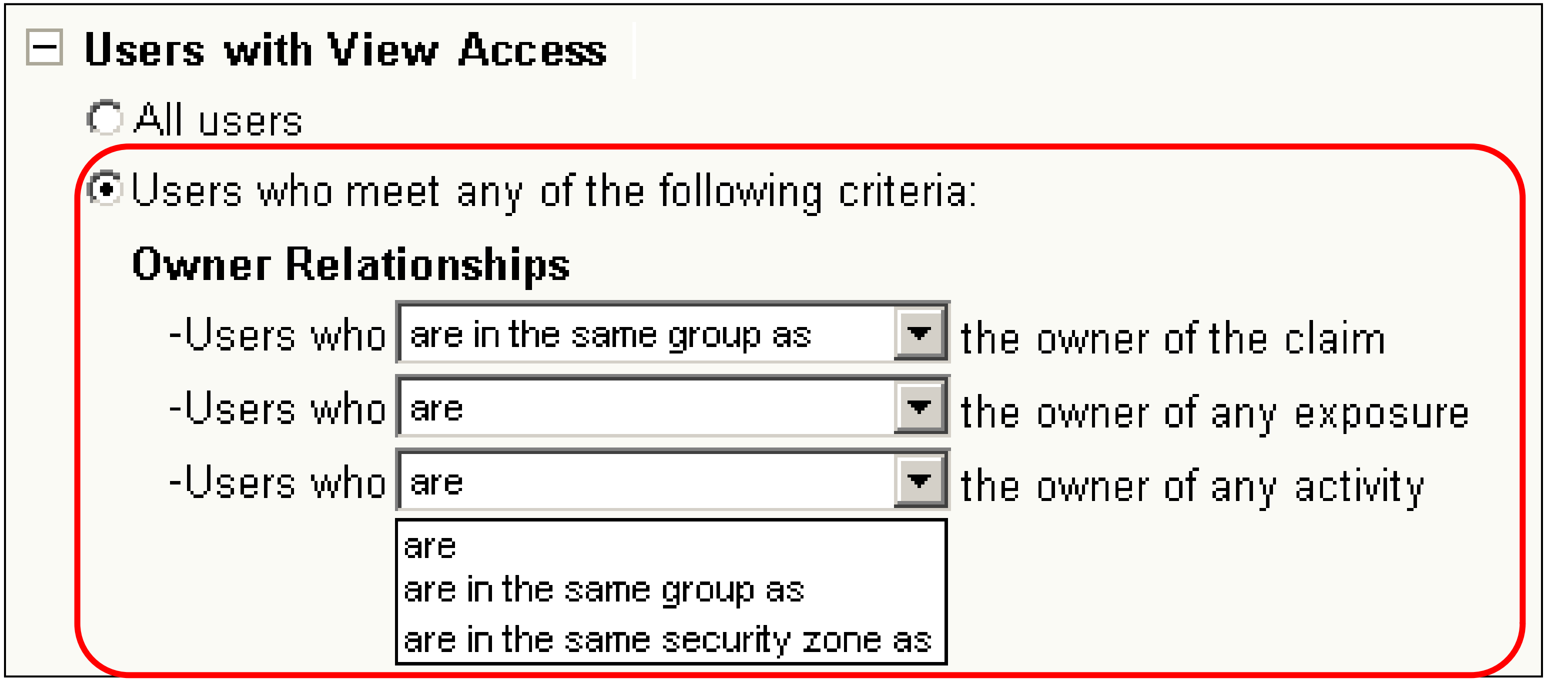
Claim User Role Relationships

Add Remove

□	* **Relationship To Role Owner**	* **Claim User Role**
□	<none selected> ▾	<none selected> ▾

- For claims with a given security type, you can open up view access to all users

View Access: Users Related to an Object Owner



⊟ **Users with View Access**

○ All users

● Users who meet any of the following criteria:

Owner Relationships

-Users who [are in the same group as ▾] the owner of the claim

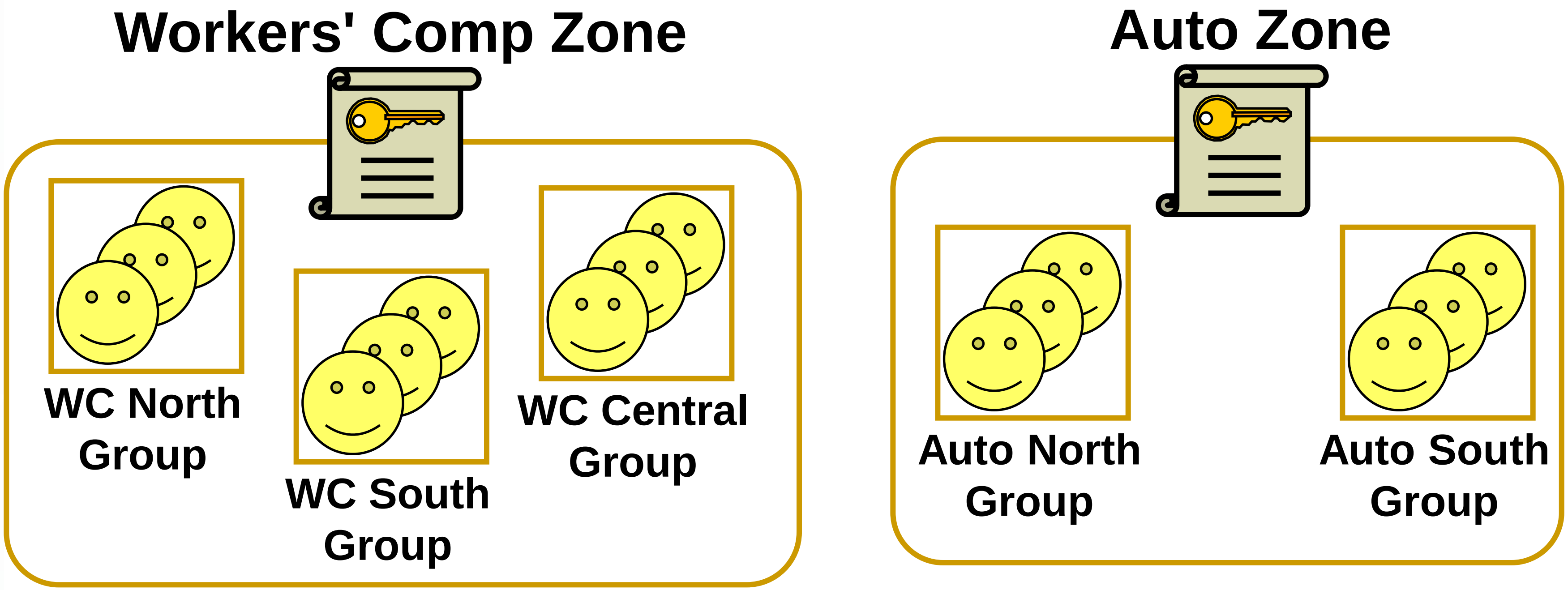
-Users who [are ▾] the owner of any exposure

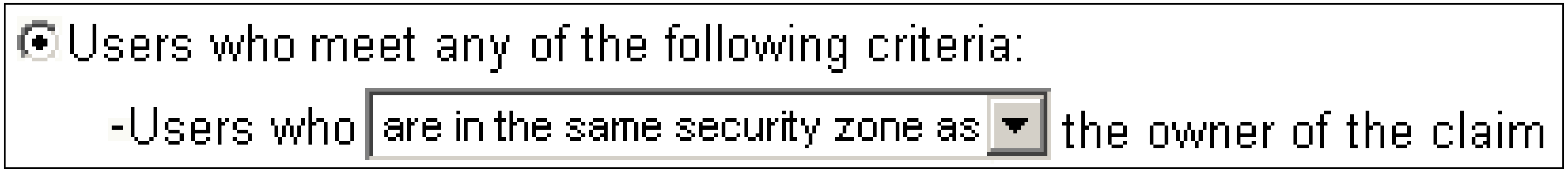
-Users who [are ▾] the owner of any activity

- You can limit view access to...:
  - ...only the owners of...
  - ...only people in the same group(s) as owners of...
  - ...only people in the same security zone(s) as owners of...

the claim and/or its exposures and/or its activities

Security Zones



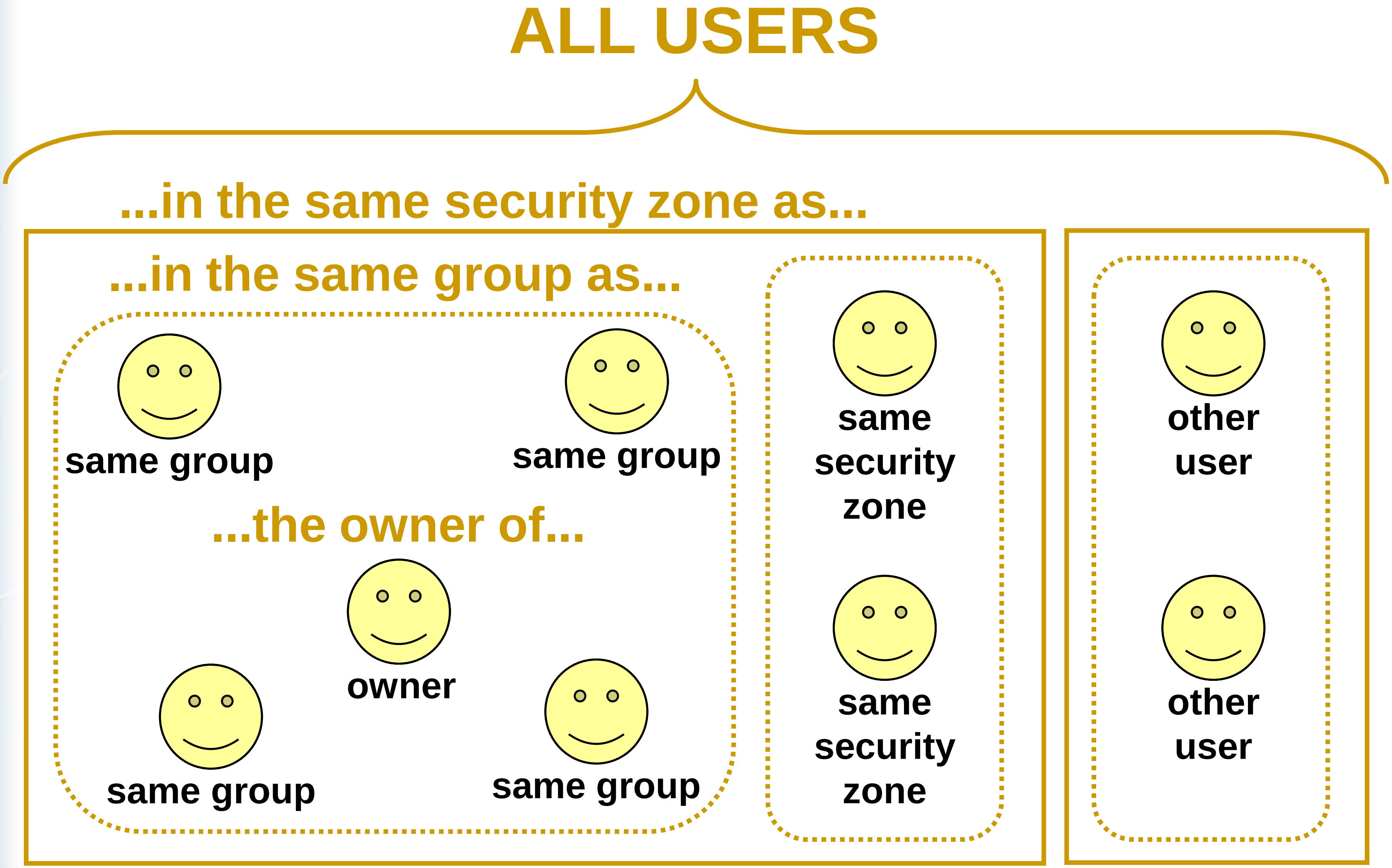


● Users who meet any of the following criteria:

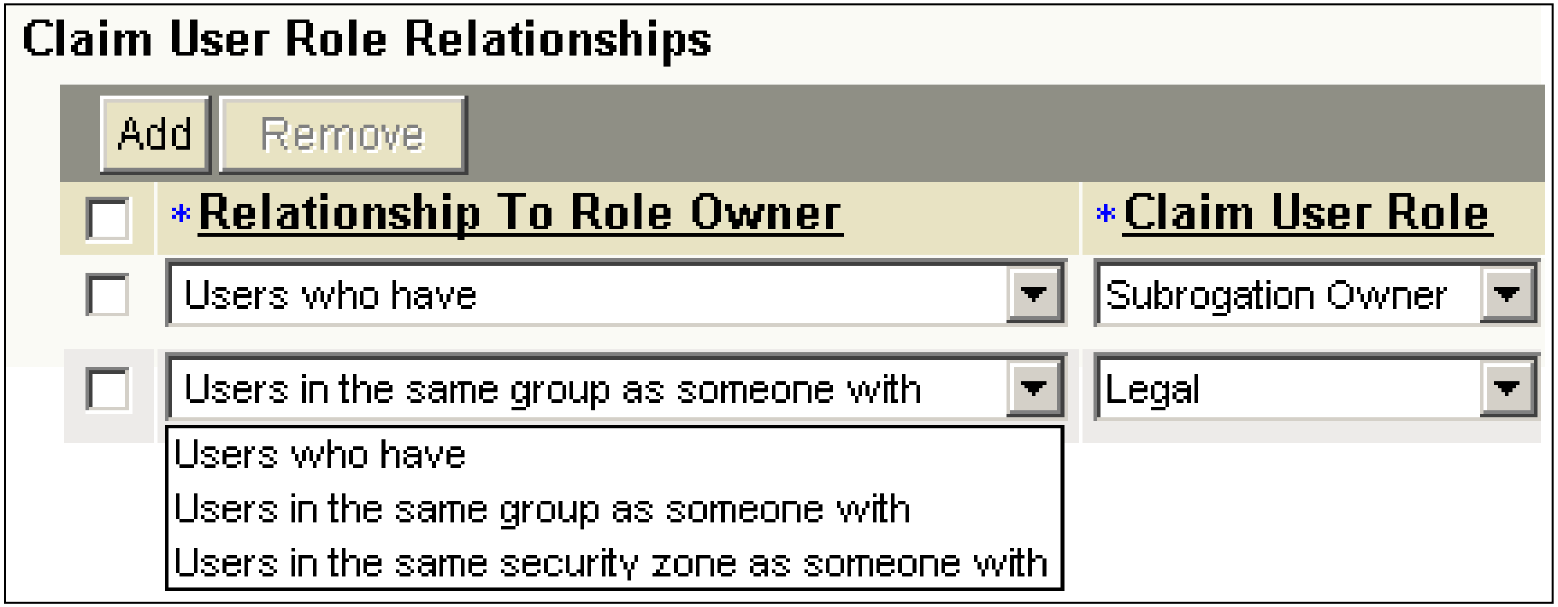
-Users who are in the same security zone as ▼ the owner of the claim

- A security zone is a collection of groups
  - Users can be given ACL-controlled access to claims owned by any user in the security zone

The Inclusive Nature of Profile Criteria



View Access: Users Related to a User with a Given Claim User Role



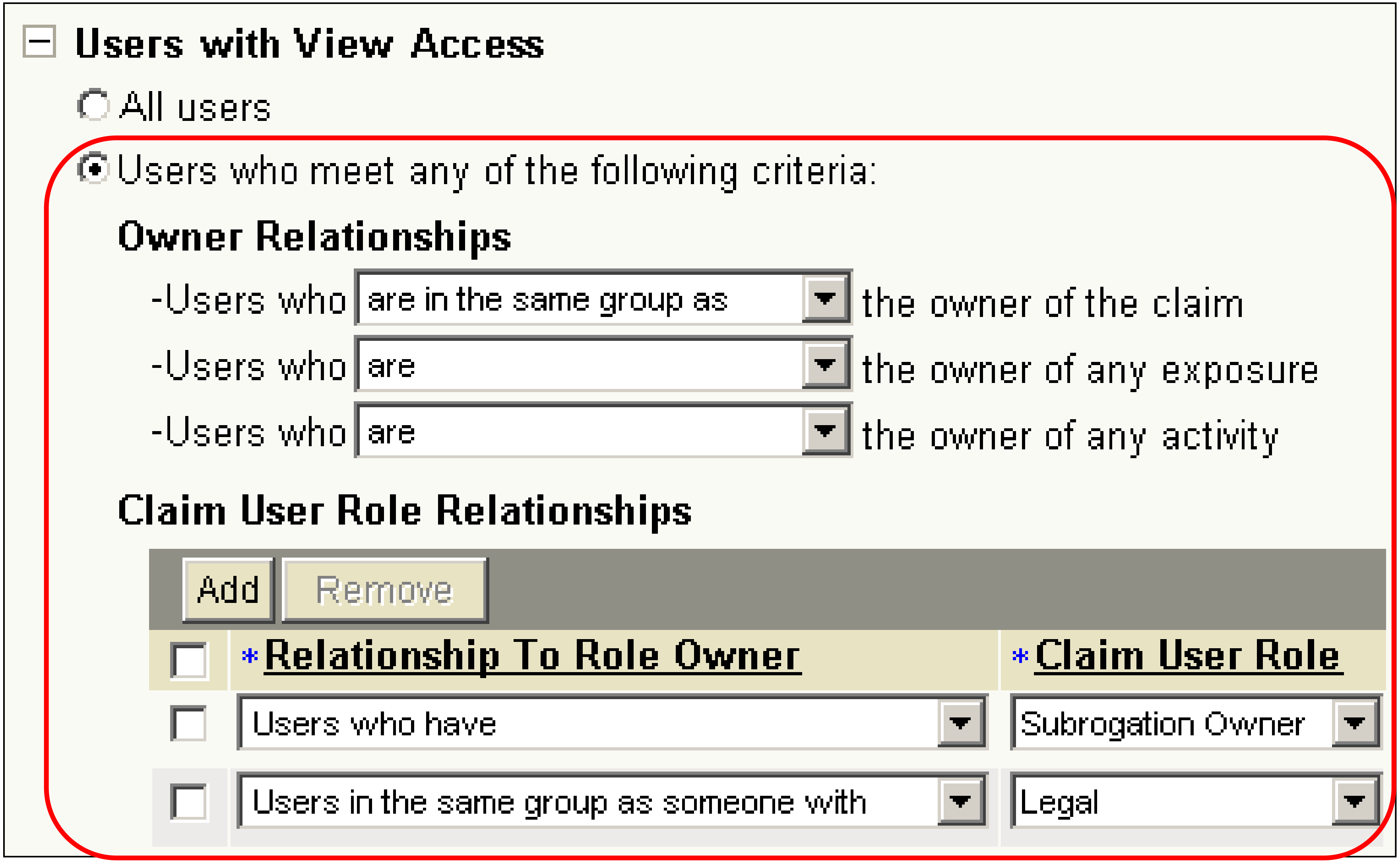
Claim User Role Relationships

□	* Relationship To Role Owner	* Claim User Role
□	Users who have	Subrogation Owner
□	Users in the same group as someone with	Legal

Users who have
Users in the same group as someone with
Users in the same security zone as someone with

- You can limit view access to...:
  - Users with a given claim user role on that claim
  - Users in the same group (or security zone) as someone with a given claim user role on that claim

View Access: Combining Ownership and Claim Role Relationships



⊟ **Users with View Access**

○ All users

● Users who meet any of the following criteria:

Owner Relationships

-Users who [are in the same group as ▾] the owner of the claim

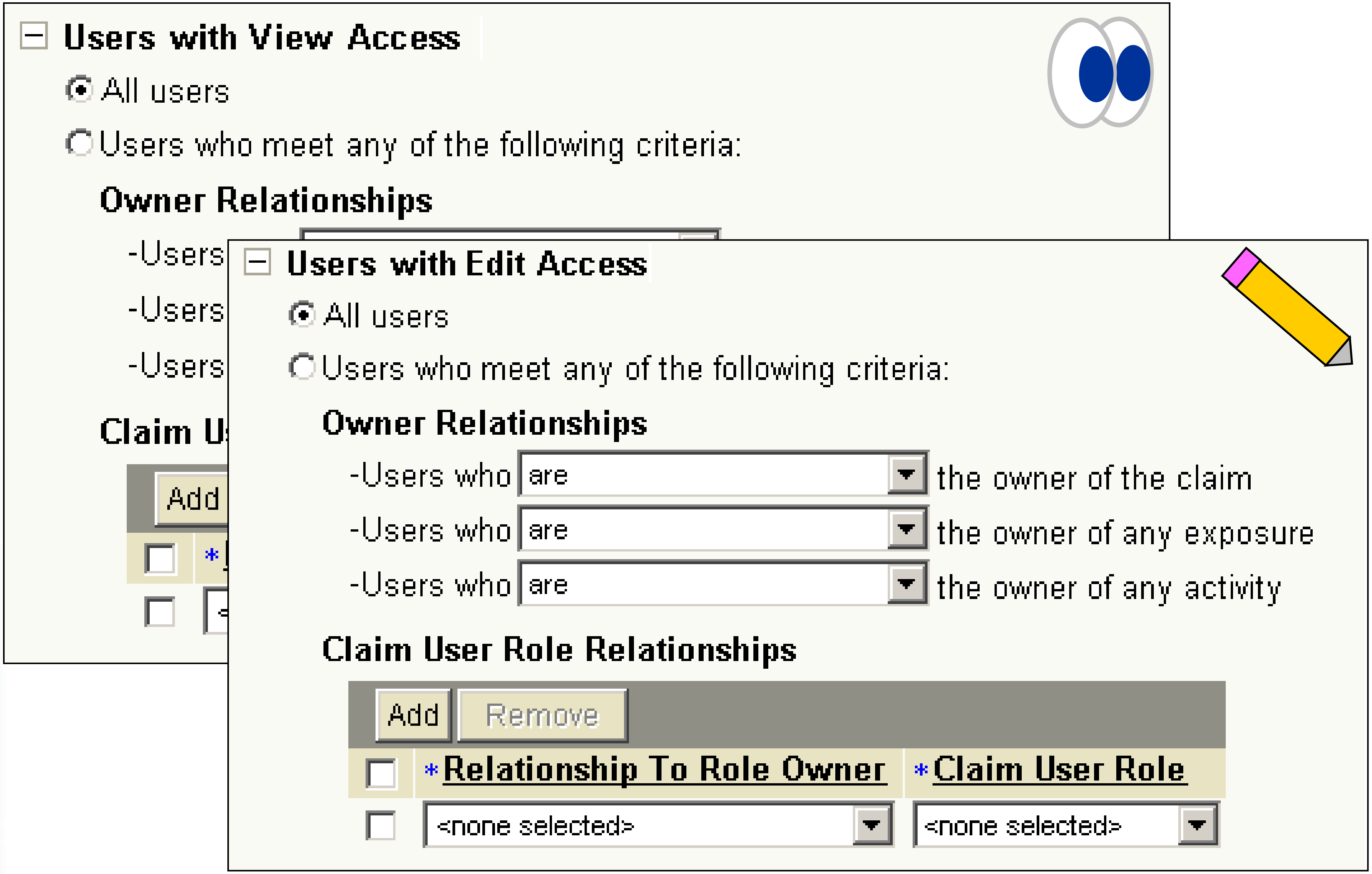
-Users who [are ▾] the owner of any exposure

-Users who [are ▾] the owner of any activity

Claim User Role Relationships

□	* Relationship To Role Owner	* Claim User Role
□	Users who have	Subrogation Owner
□	Users in the same group as someone with	Legal

Edit Access Has the Same Options As View Access



⊟ Users with View Access

● All users

○ Users who meet any of the following criteria:

Owner Relationships

-Users

-Users

-Users

Claim U

Add

□ *

□

⊟ Users with Edit Access

● All users

○ Users who meet any of the following criteria:

Owner Relationships

-Users who [are ▼] the owner of the claim

-Users who [are ▼] the owner of any exposure

-Users who [are ▼] the owner of any activity

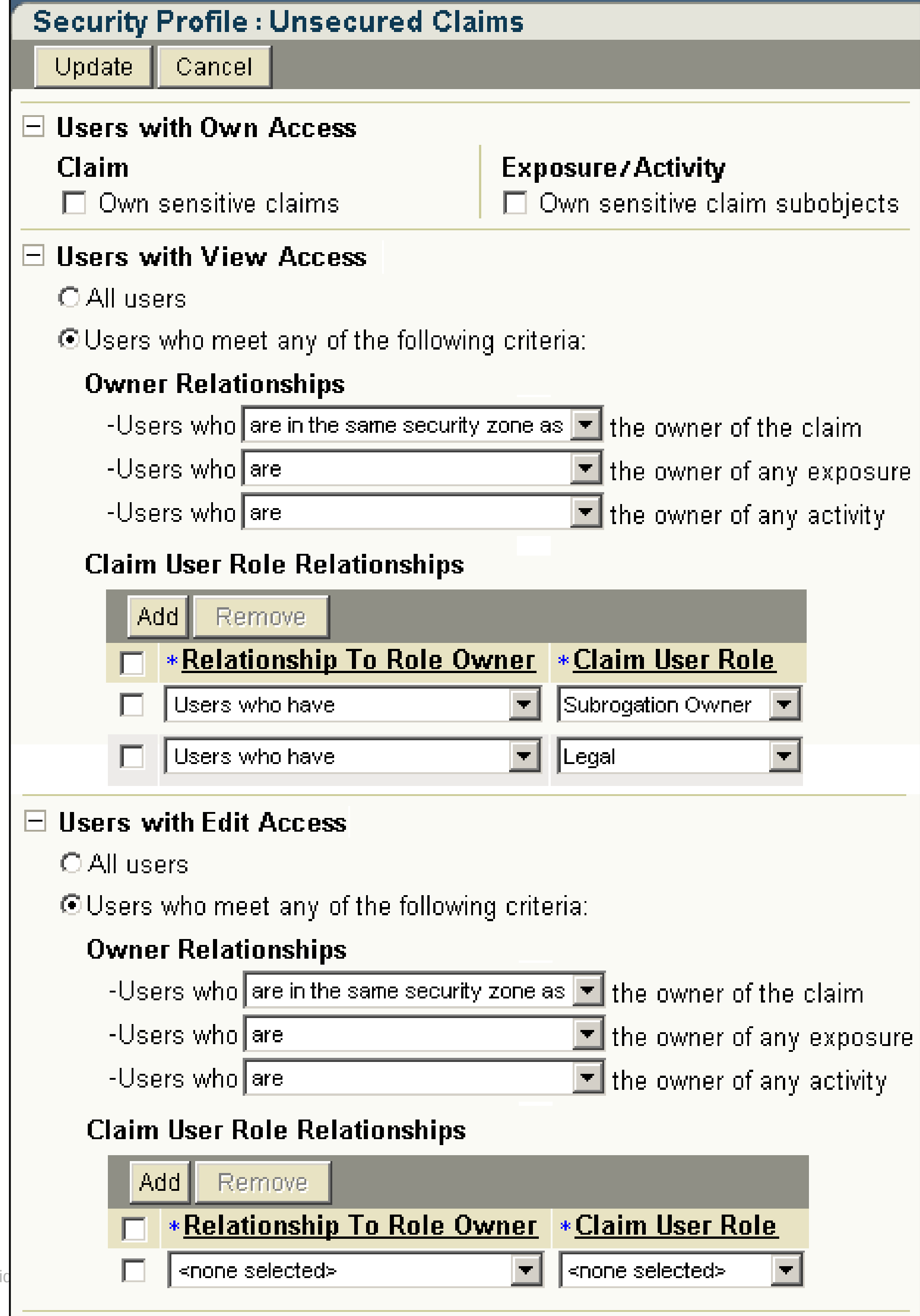
Claim User Role Relationships

Add | Remove

□	* Relationship To Role Owner	* Claim User Role
□	<none selected> ▼	<none selected> ▼

Security Profile Example: Unsecured Claims

- No ownership restrictions
- To view, you must either:
  - Be in the same security zone as the claim owner
  - Be a sub-object owner
  - Have the "subrogation owner" or "legal" role on the claim
- To edit, you must be in the same security zone as the claim owner (or be an exposure or activity owner)



Security Profile : Unsecured Claims

Update | Cancel

⊟ Users with Own Access

Claim
□ Own sensitive claims

Exposure/Activity
□ Own sensitive claim subobjects

⊟ Users with View Access

○ All users
● Users who meet any of the following criteria:

Owner Relationships

-Users who [are in the same security zone as ▾] the owner of the claim
-Users who [are ▾] the owner of any exposure
-Users who [are ▾] the owner of any activity

Claim User Role Relationships

Add | Remove

□	*Relationship To Role Owner	*Claim User Role
□	Users who have ▾	Subrogation Owner ▾
□	Users who have ▾	Legal ▾

⊟ Users with Edit Access

○ All users
● Users who meet any of the following criteria:

Owner Relationships

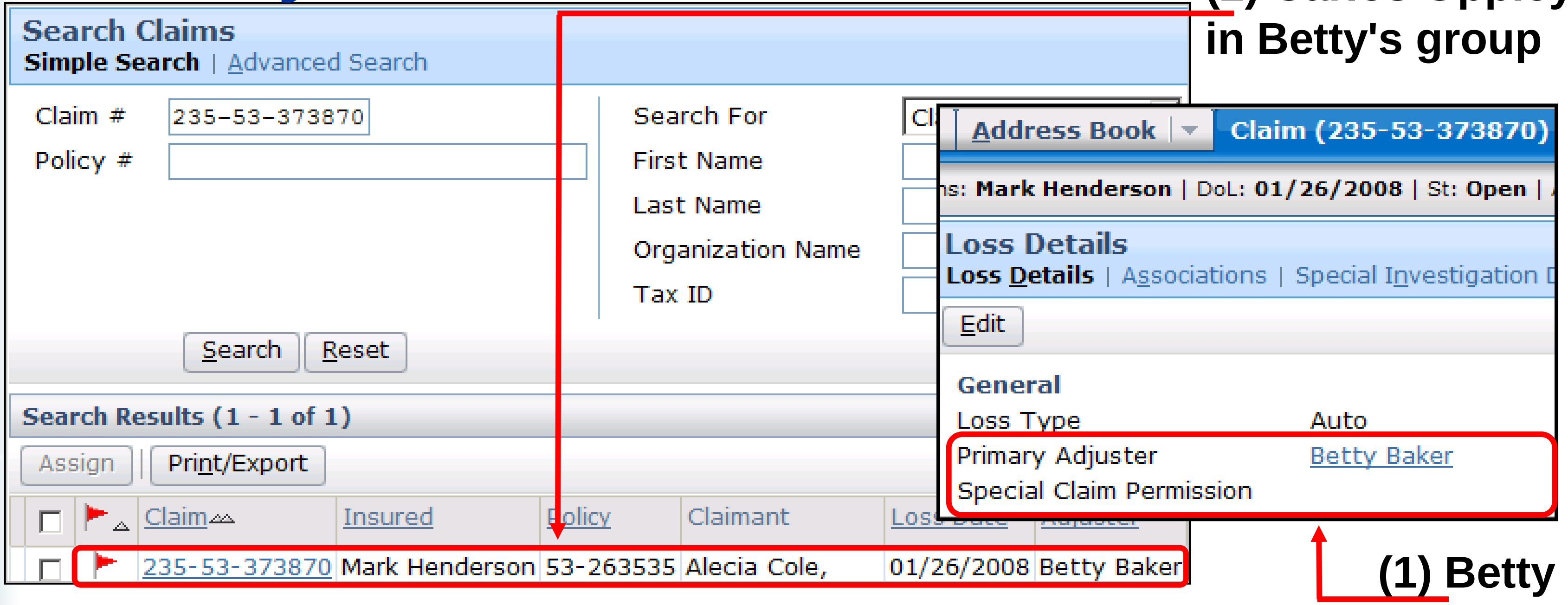
-Users who [are in the same security zone as ▾] the owner of the claim
-Users who [are ▾] the owner of any exposure
-Users who [are ▾] the owner of any activity

Claim User Role Relationships

Add | Remove

□	*Relationship To Role Owner	*Claim User Role
□	<none selected> ▾	<none selected> ▾

Security Profile in Action



Search Claims

Simple Search | Advanced Search

Claim #	235-53-373870	Search For	Cl
Policy #		First Name	
		Last Name	
		Organization Name	
		Tax ID	

Search Results (1 - 1 of 1)

□		Claim	Insured	Policy	Claimant	Loss Date	Adjuster
□		235-53-373870	Mark Henderson	53-263535	Alecia Cole,	01/26/2008	Betty Baker

ns: **Mark Henderson** | DoL: **01/26/2008** | St: **Open** |

Loss Details

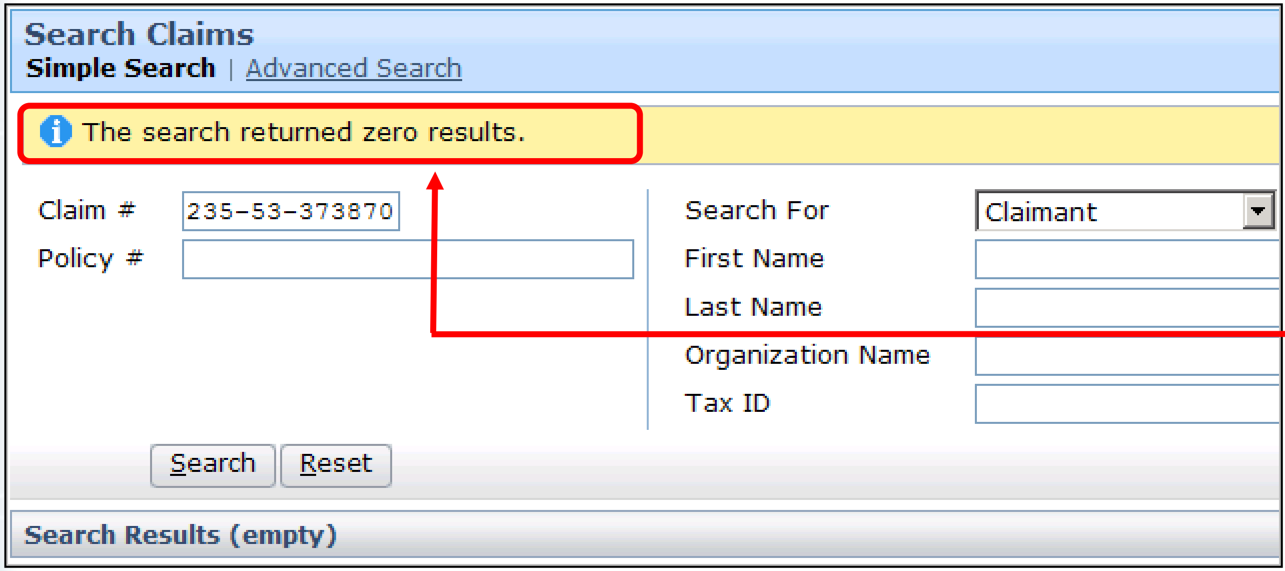
Loss Details | Associations | Special Investigation D

General

Loss Type	Auto
Primary Adjuster	Betty Baker
Special Claim Permission	

(2) Carlos Oppley is in Betty's group

(1) Betty Baker owns this unsecured claim



Search Claims

Simple Search | Advanced Search

The search returned zero results.

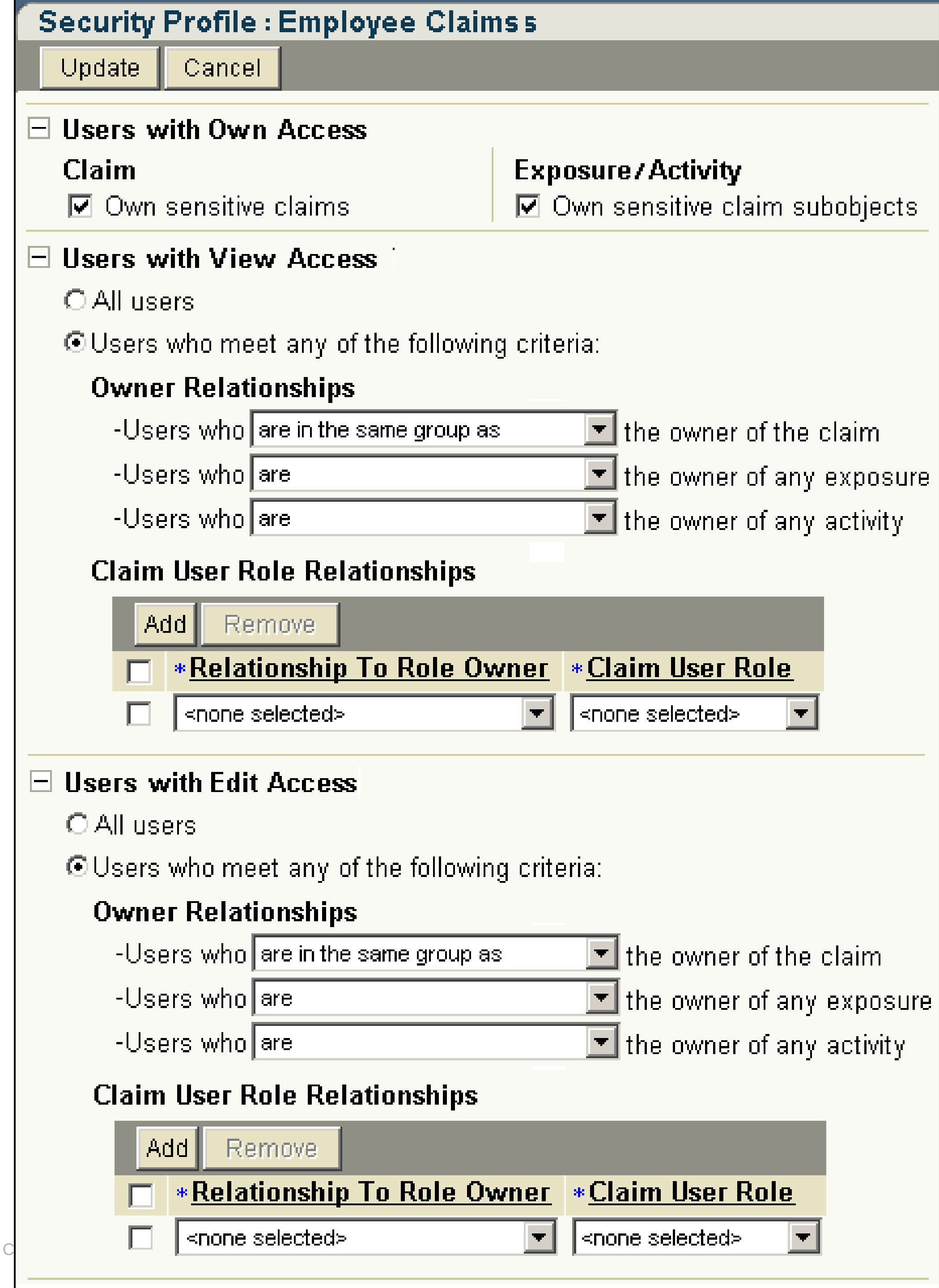
Claim #	235-53-373870	Search For	Claimant
Policy #		First Name	
		Last Name	
		Organization Name	
		Tax ID	

Search Results (empty)

(3) Gerald Ickes is a workers' comp adjuster outside Betty's security zone

Security Profile Example: Employee Claims

- To own a claim, you must have "own sensitive claims" permission
- To own a sub-object, you must have "own sensitive subobjects" permission
- To view or edit it, you must either:
  - Be in the same group as the claim owner
  - Own an exposure or activity on the claim



Security Profile : Employee Claims s

⊟ Users with Own Access

Claim	Exposure/Activity
☑ Own sensitive claims	☑ Own sensitive claim subobjects

⊟ Users with View Access

○ All users

● Users who meet any of the following criteria:

Owner Relationships

-Users who are in the same group as the owner of the claim

-Users who are the owner of any exposure

-Users who are the owner of any activity

Claim User Role Relationships

□	*Relationship To Role Owner	*Claim User Role
□	<none selected>	<none selected>

⊟ Users with Edit Access

○ All users

● Users who meet any of the following criteria:

Owner Relationships

-Users who are in the same group as the owner of the claim

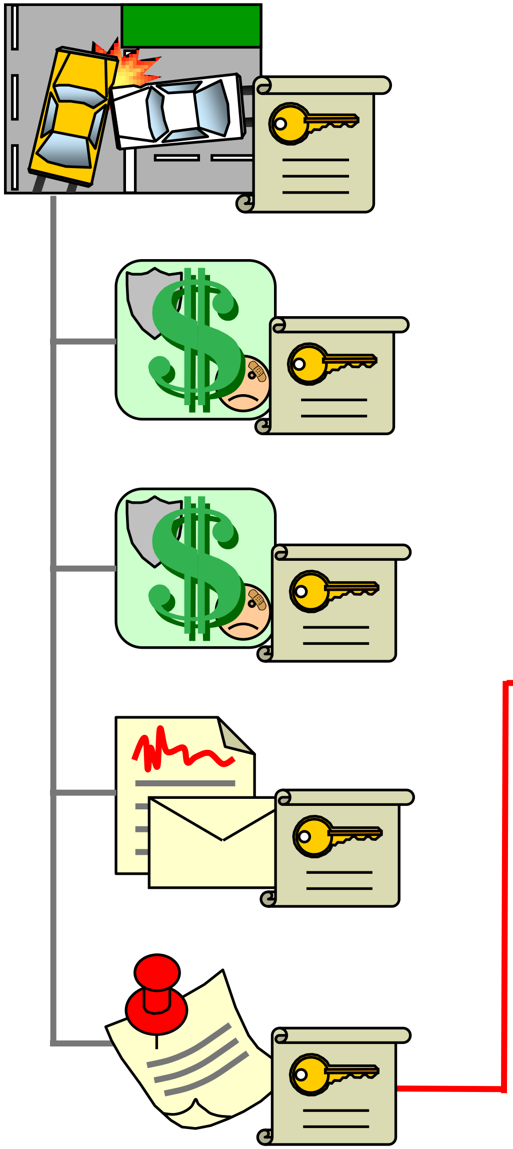
-Users who are the owner of any exposure

-Users who are the owner of any activity

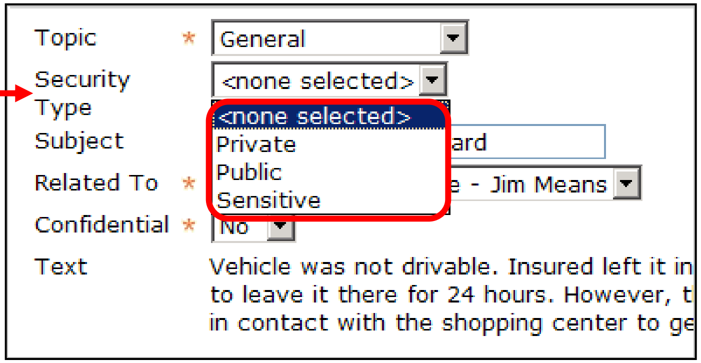
Claim User Role Relationships

□	*Relationship To Role Owner	*Claim User Role
□	<none selected>	<none selected>

ACLs for Exposures, Documents and Notes



- In some cases, access needs to be restricted for levels more granular than the claim level
  - ACL access for exposures, notes and documents is similar to that of claim-level ACLs
  - Documents and Notes have a visible security type field that may be set

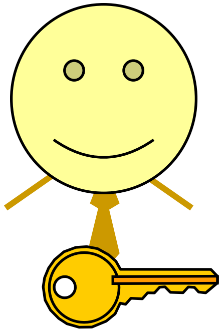


Topic	*	General
Security Type		<none selected>
Subject		ard
Related To	*	e - Jim Means
Confidential	*	No
Text		Vehicle was not drivable. Insured left it in to leave it there for 24 hours. However, t in contact with the shopping center to ge

<none selected>
Private
Public
Sensitive

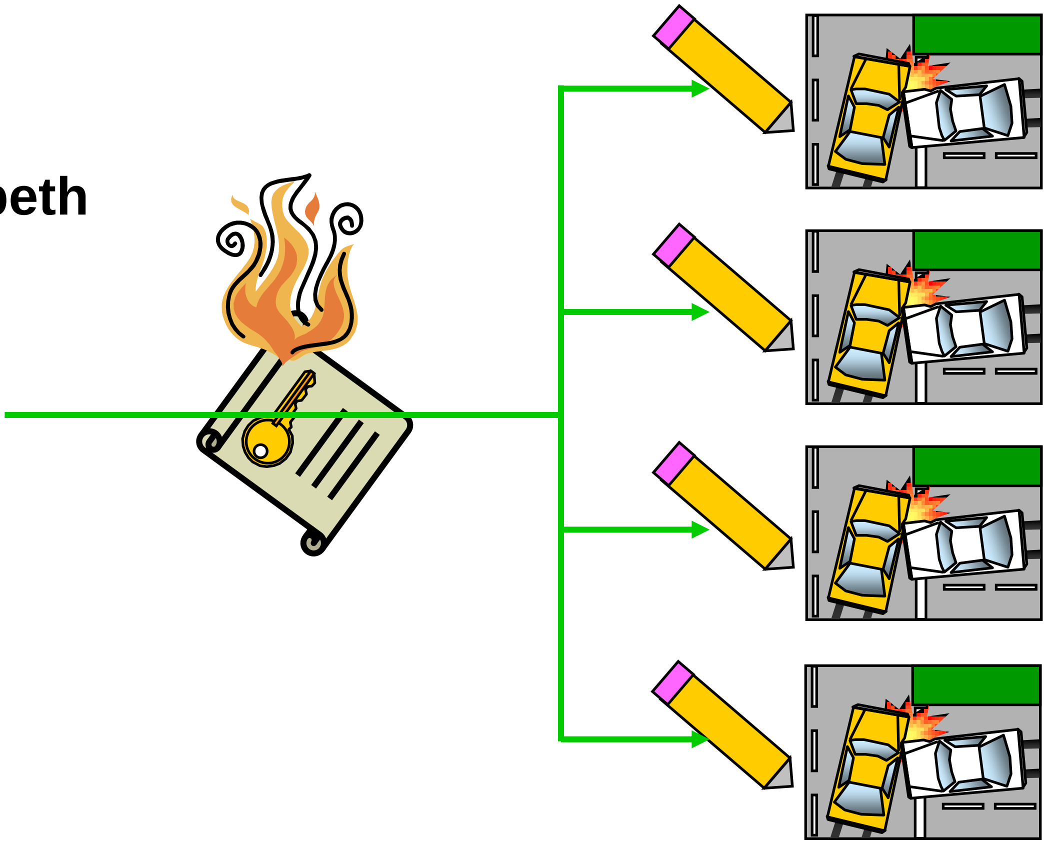
  - Exposure security type is typically set during setup

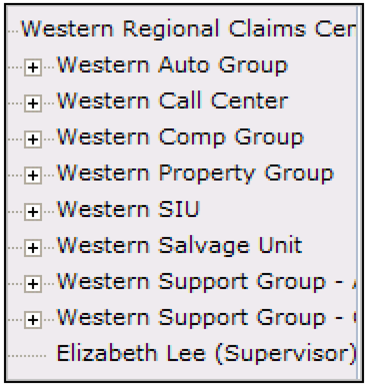
The Ignore ACLS System Permission



Elizabeth Lee

Ignore ACLs

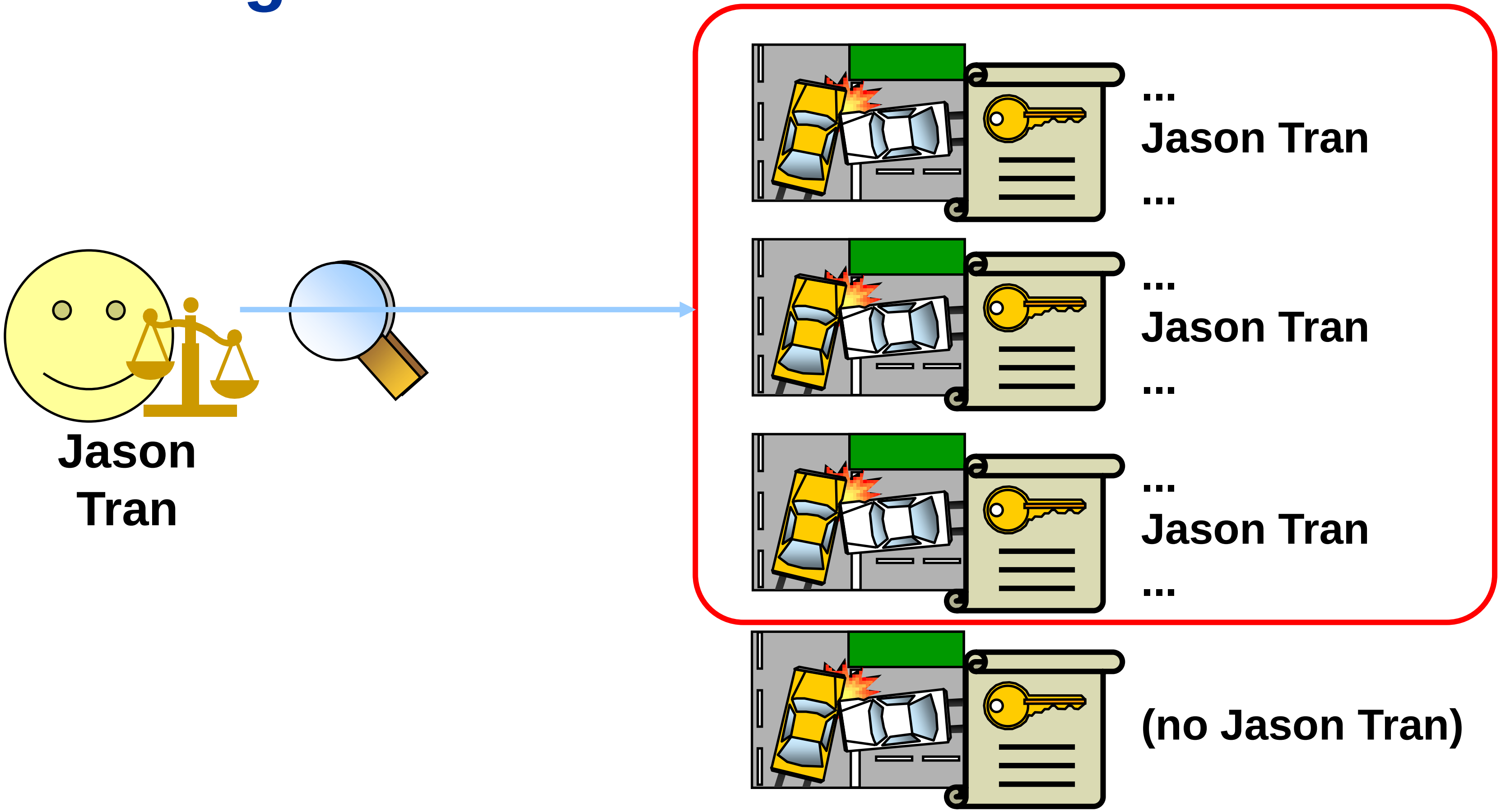




Western Regional Claims Cer
- Western Auto Group
- Western Call Center
- Western Comp Group
- Western Property Group
- Western SIU
- Western Salvage Unit
- Western Support Group - /
- Western Support Group - (
- Elizabeth Lee (Supervisor)

- There is a system permission called "Ignore ACLs" which lets a user view and edit claims without regards to ACLs

Restricting Searches



- You can configure ClaimCenter searches so that they only return objects a user has ACL-based access to

Lesson Objectives Review

You should now be able to:

- Describe the role of permissions in controlling access
- Assign permissions to users
- Describe how non-claim-centric permissions work to provide "all or nothing" access
- Describe how Access Control Lists (ACLs) provide access to some but not all claims

Review Questions

1. A given user appears on the access control list for claim 234-22-147282, but that user cannot view or edit the claim. How could this happen?
2. A security profile can specify criteria for three types of access. What are the three types of access?
3. Two different claims that use the same security profile can have two completely different access control lists. Why?
4. What is the business motivation for having multiple security profiles?
5. What is a security zone used for?
6. A security profile can restrict view access to a given type of claim using up to four types of criteria. Three of them pertain to ownership (the claim owner, exposure owners, activity owners). What does the fourth criteria pertain to?

Reservation of Rights