

# Security Label Authorization in Directory Services

Kurt Zeilenga



# Authorization Flavors

## ◆ Identity-based

- users
- groups

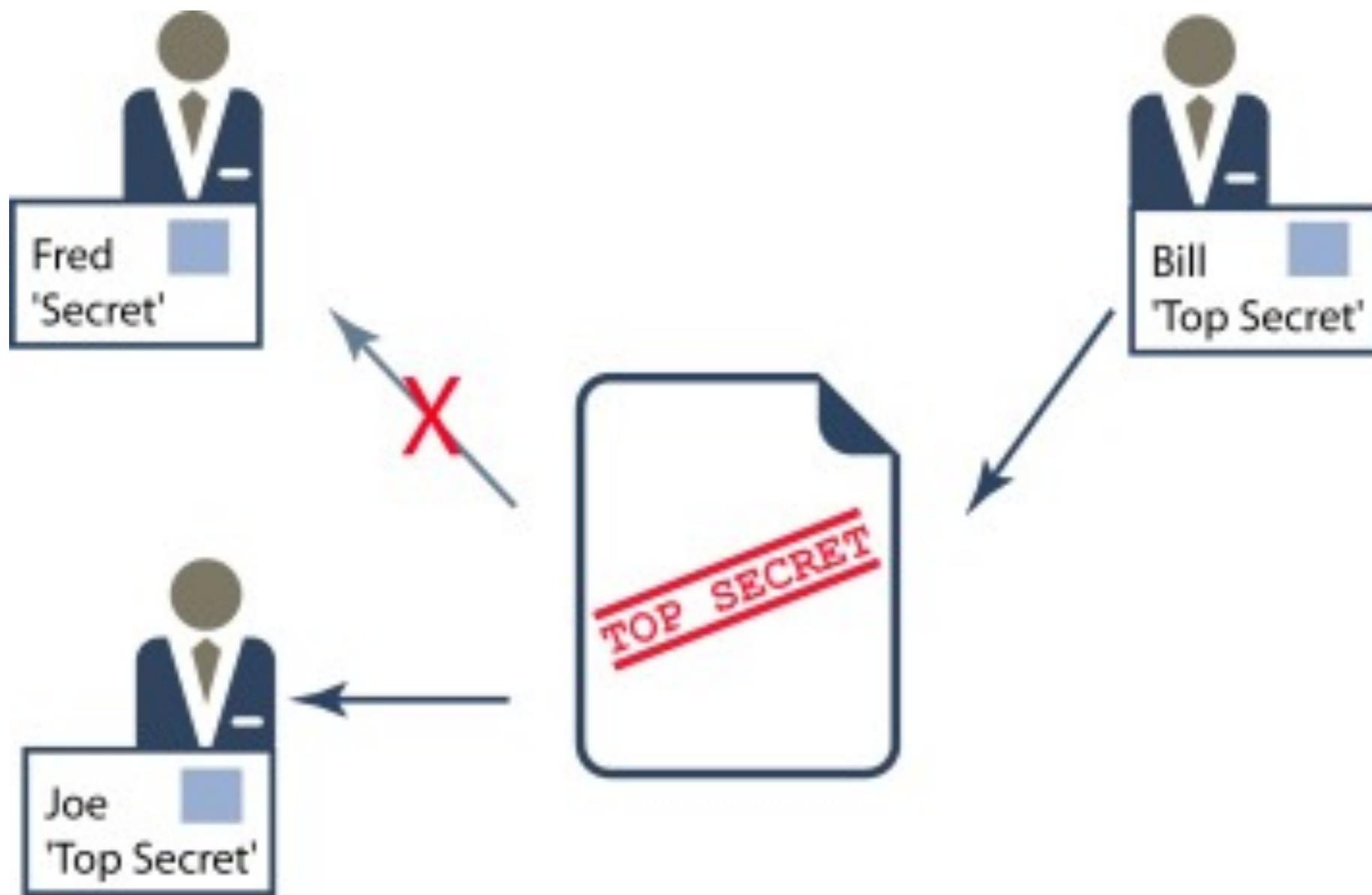
## ◆ Role-based

- Roles and occupants

## ◆ Sensitive-based (security-label based)

# Sensitive-based Authz

- ◆ authorization based upon a classification/ categorization of the sensitivity of the subject material and a user's authorization to handle information under various classes/categories of information sensitivities
- ◆ also known as “Rule-based access controls” (RBAC).
- ◆ a form of “Mandatory Access Controls”

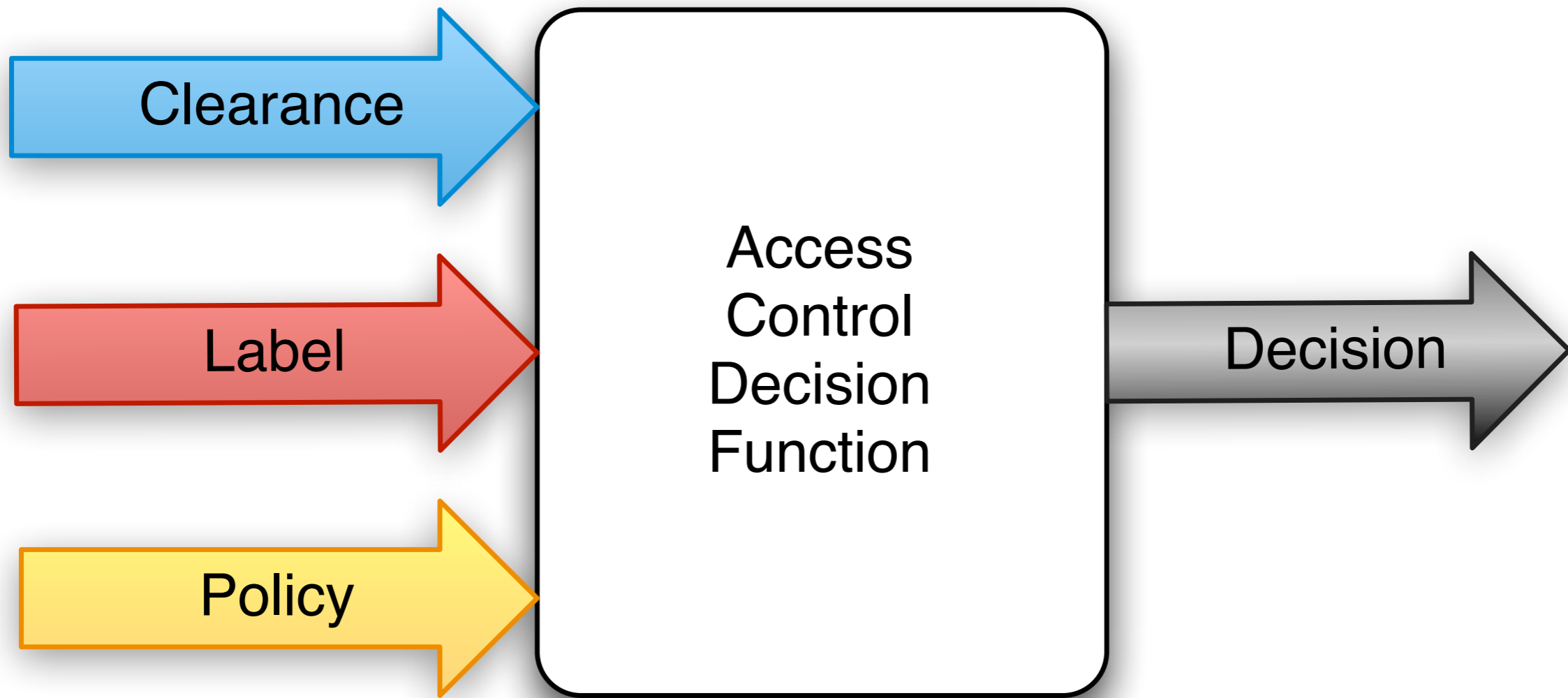


# What is an (electronic) Security Label?

- ◆ A structured representation of the sensitivity of a piece of information
- ◆ Traditionally, labels are securely bound to the piece of information through a digital signature. However, some systems use non-securely bound labels.

# What is a (electronic) clearance?

- ◆ A structured representation of an entity's (person, device, etc.) authorization to access particular information sensitivities.
- ◆ Traditionally, clearances are securely bound to the entity via an attribute certificate.



# Classes vs. Categories

- ◆ Classes are horizontal divisions of sensitivity and have a hierarchy.
  - E.g., Unclassified, Restricted, Secret
- ◆ Categories are vertical divisions of sensitivity.
  - Categories can be Restrictive, Permissive, or Informative
  - E.g., Atomic, ComSec, No Foreigner, Rel. US/UK, FOUO
- ◆ Example Label: SECRET//NOFORN
- ◆ Example Clearance:
  - Classes: Secret, Confidential, Unclassified
  - Categories: NOFORN, REL US/UK/NATO,

## Label

Policy Id

Classification

Privacy  
Mark

Security  
Categories

## Clearance

Policy Id

Classification  
Set

Security  
Categories

## Policy

Policy Id

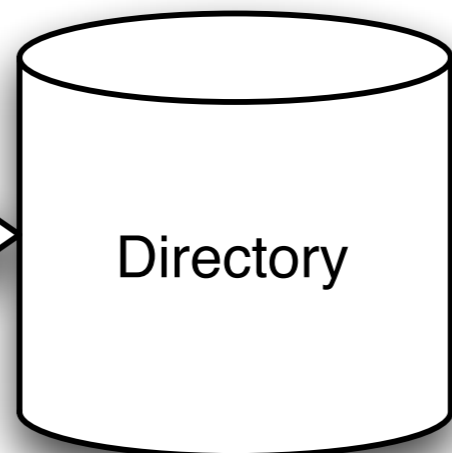
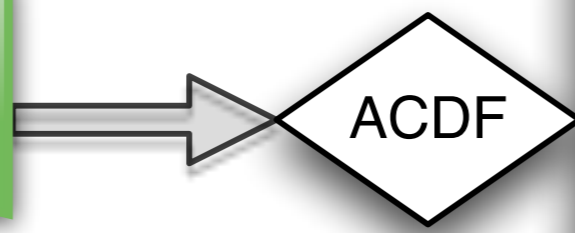
Classification  
Data

Security  
Categories  
Data


Jane  
Top Secret




Secret



Mary  
Unclassified



Beth  
Secret



# But why?