

TIED ABAC Advances Since GEC12

Ted Faber, Mei-Hui Su, Mike Ryan
{faber,mei,mikeryan}@isi.edu

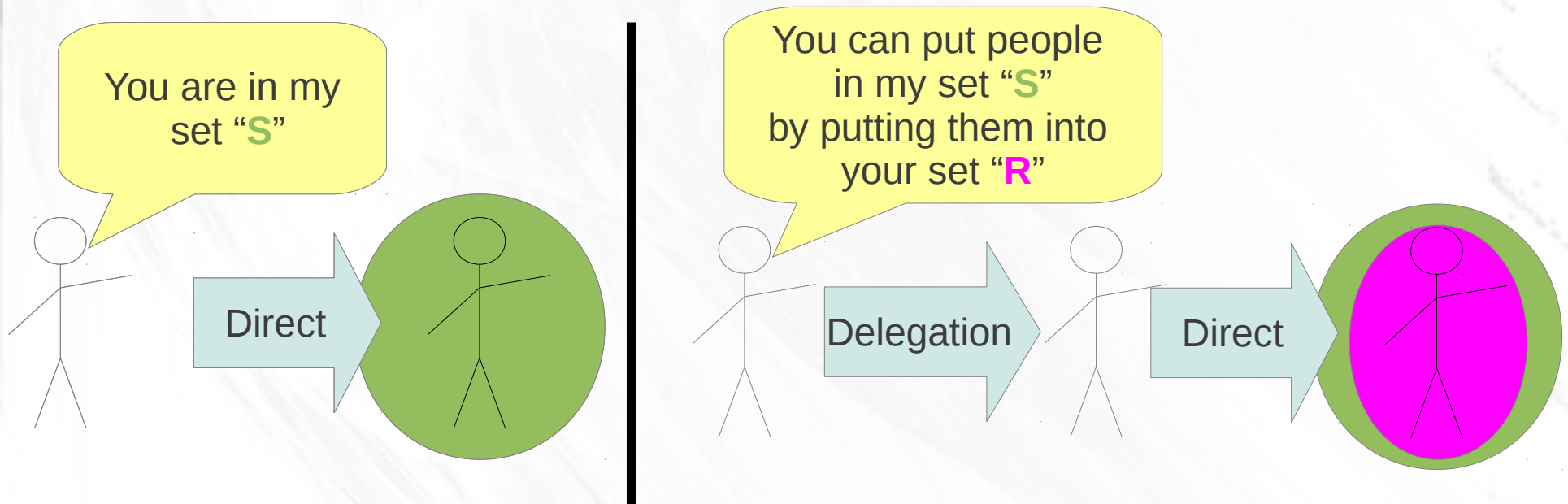
13 Mar 2012

Two Areas Of Work

- RT2 Logic Support
 - What's RT2?
 - RT0 (logic from last GEC) → RT2 (today)
 - Show expressive power
 - **New**: support for RT2 in libraries
- New Tools (RT0): **Demo Session**
 - Administrator-driven and User-driven tools
 - Easier to visualize large policies vs. Crudge
 - Early Natural Language interpretation

RT0: Assigning Principals to Sets

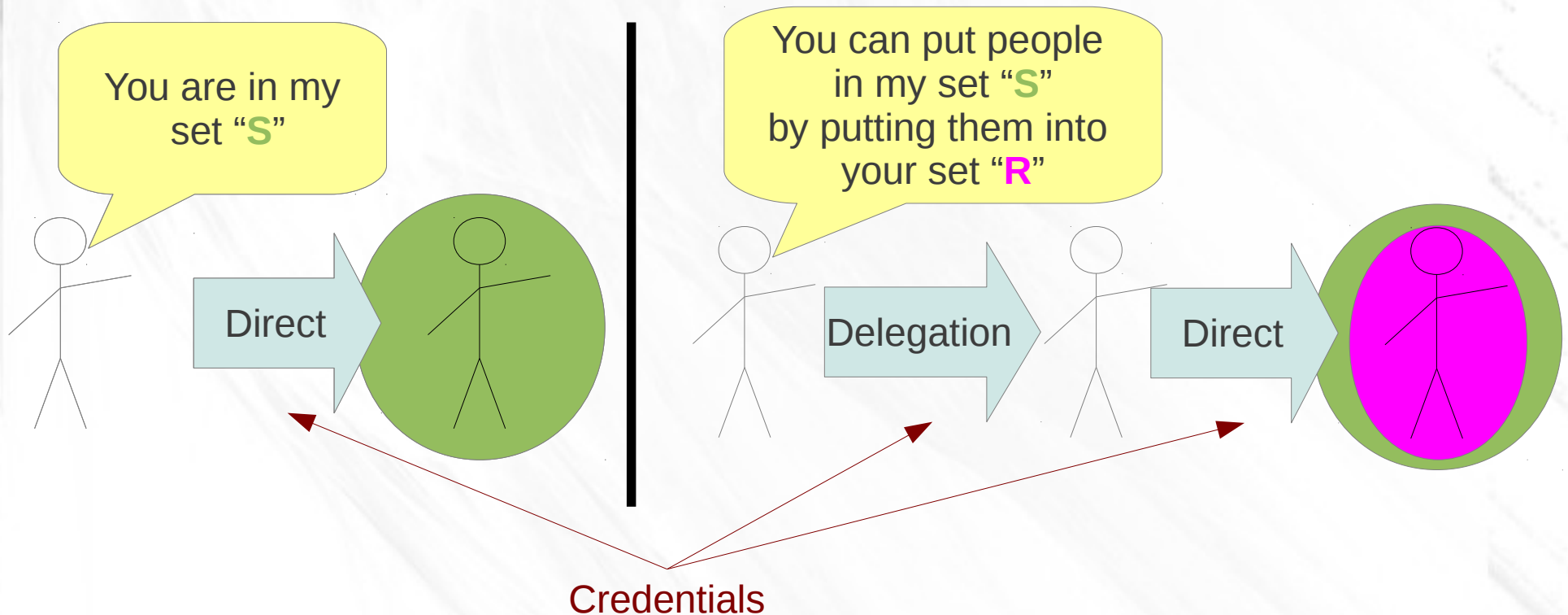
Or giving roles to principals...



Privileges are granted to members of a set/role

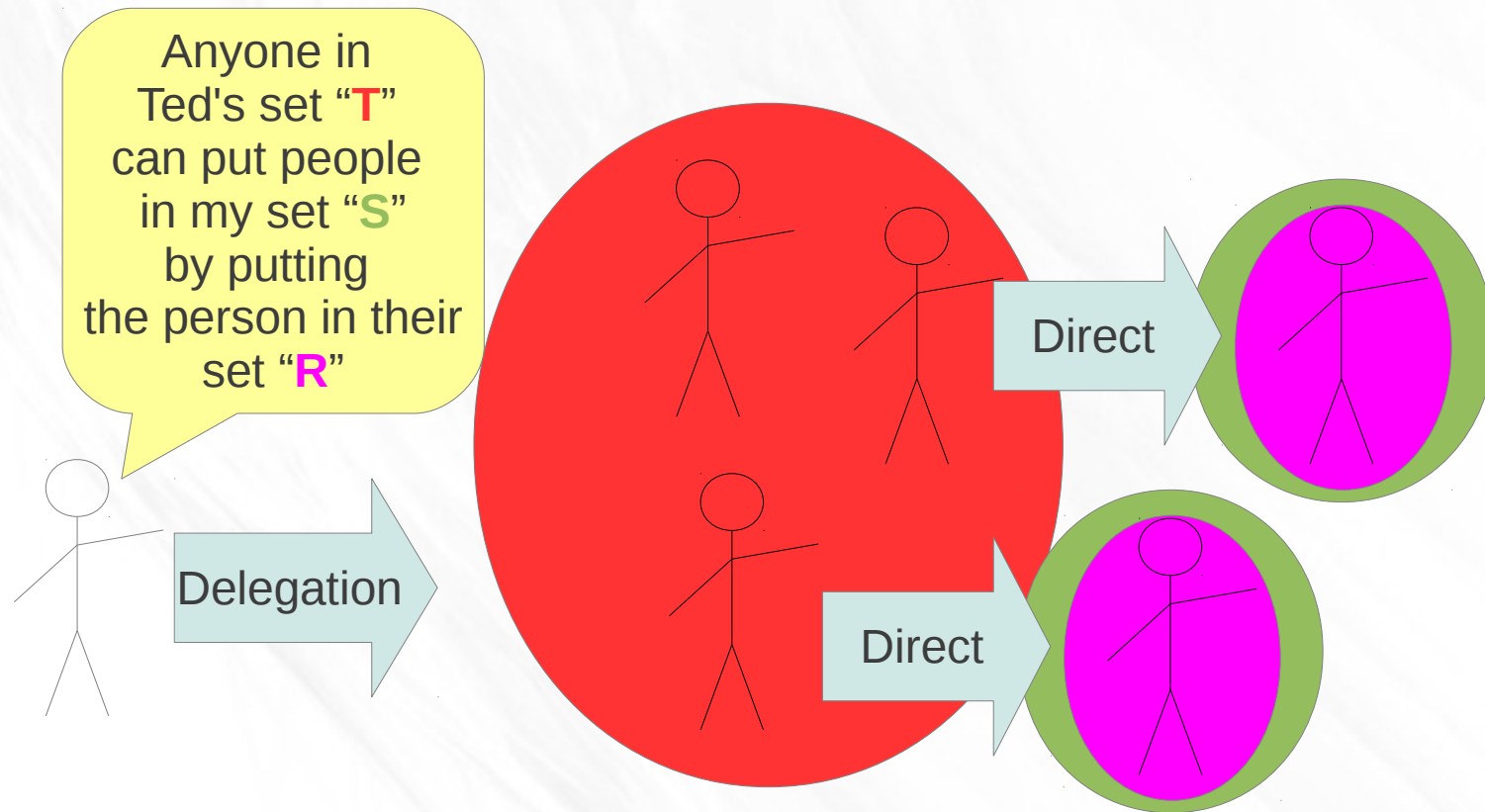
RT0: Assigning Principals to Sets

Or giving roles to principals...

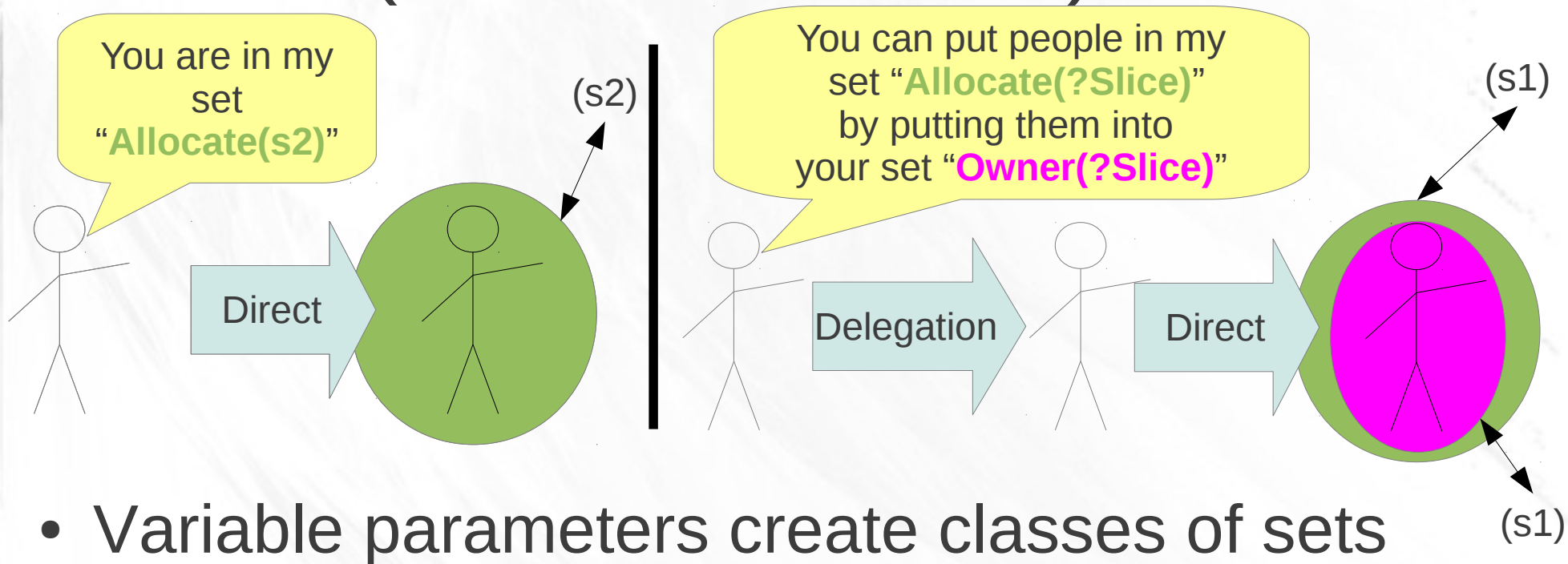


Privileges are granted to members of a set/role

RT0: Assigning Principals to Sets



RT1: Tying Data To Sets (Parameterization)



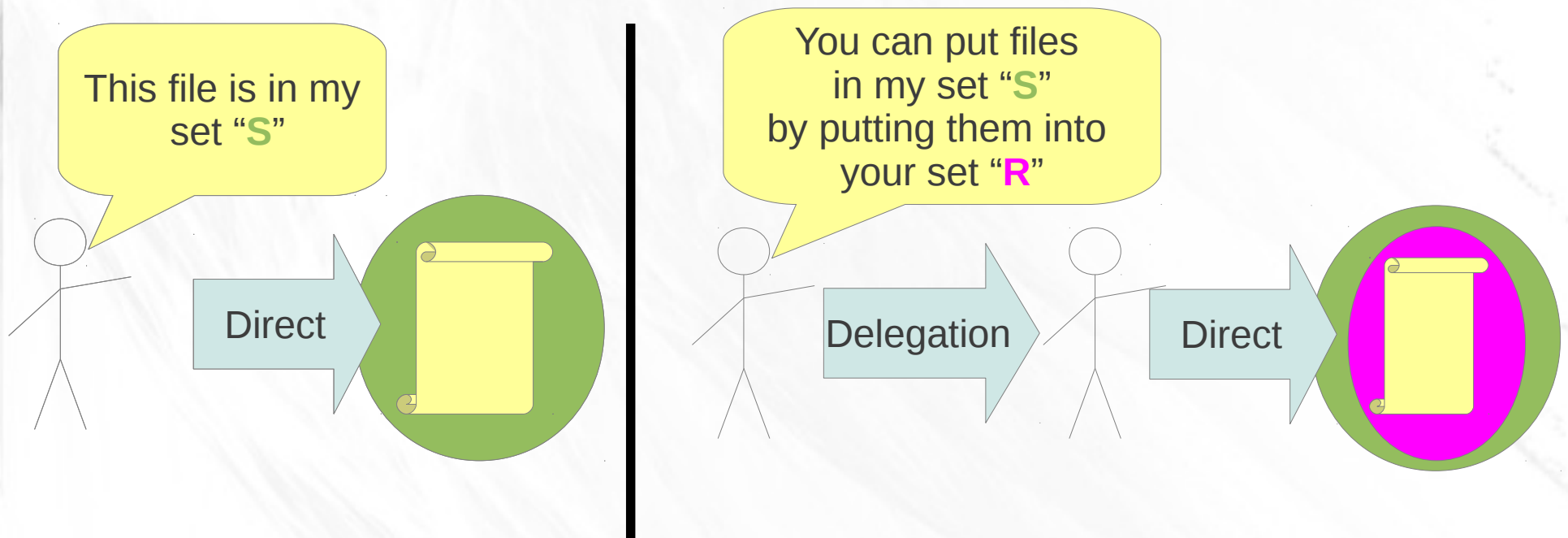
- Variable parameters create classes of sets
 - *?name* is a variable parameter
 - Each **Owner(Slicename)** assignment creates a distinct **Allocate(Slicename)** set

RT1: Constraining Parameters

- Variables be constrained
 - ?X:[0...10] – constrained integer
 - ?P:[Ted, Bob] – constrained person
 - ?slicename: [slice1,slice2] – constrained string
- Constraints are static
 - defined at delegation time

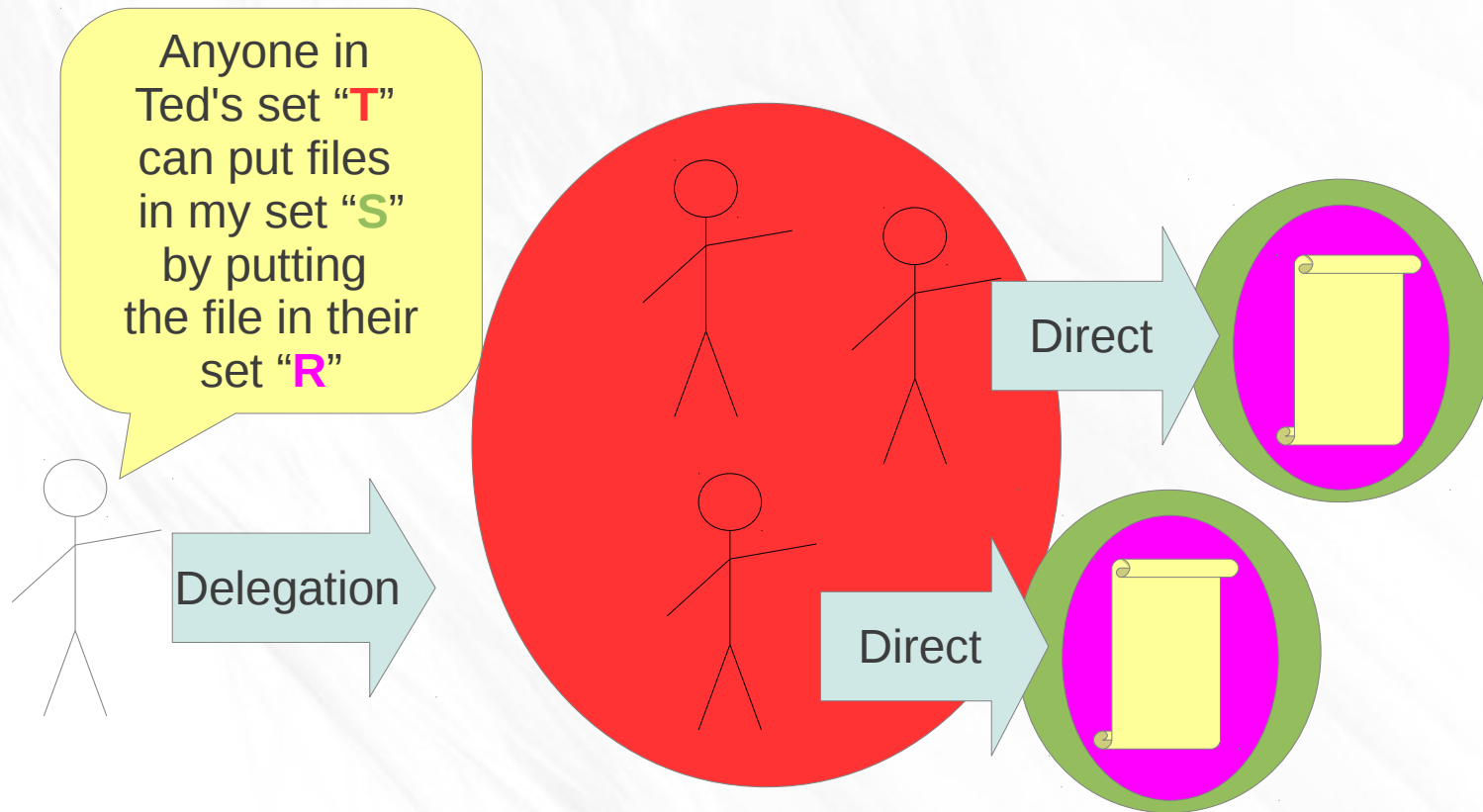
Constrained Parameter Binding
Is a Big Step Up

RT2: Put objects/data into Object Sets



- Objects can be any valid RT1 parameters
- Object sets are typed
- Object sets may be parameterized

RT2: Putting Objects/Data into Object Sets



RT2: object sets can be constraints!

- Object set constraints: dynamic constraints
 - ?S:[GPO.slices] – slices that are GPO slices
- Express dynamic permissions on objects
 - Shutdown(?slice:[GPO.slices]) set/role
 - Set of people who can “shutdown GPO slices”
 - **Object set constraint** on **role parameter**
- RT2 represents a sweet spot for expression

RT2 Status

- Extended libabac to work with RT2
 - Include higher power proving engine
 - Parameter binding and constraints
 - Extend credential syntax for new concepts
 - Maintain existing interfaces
- There is an alpha library release
 - `git clone -b rt2 git://abac.deterlab.net/abac.git`