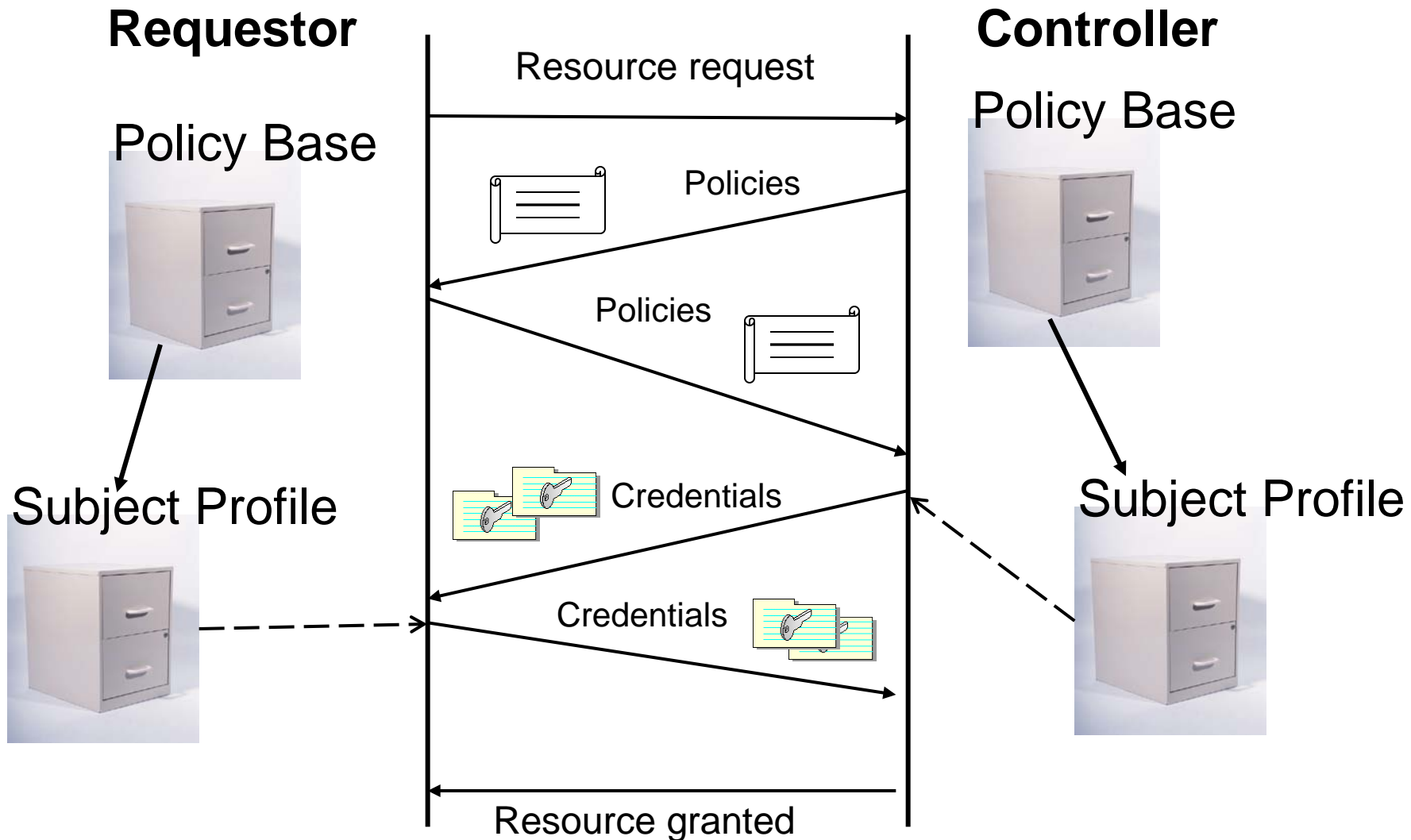


Automatic Trust Negotiation

Motivation

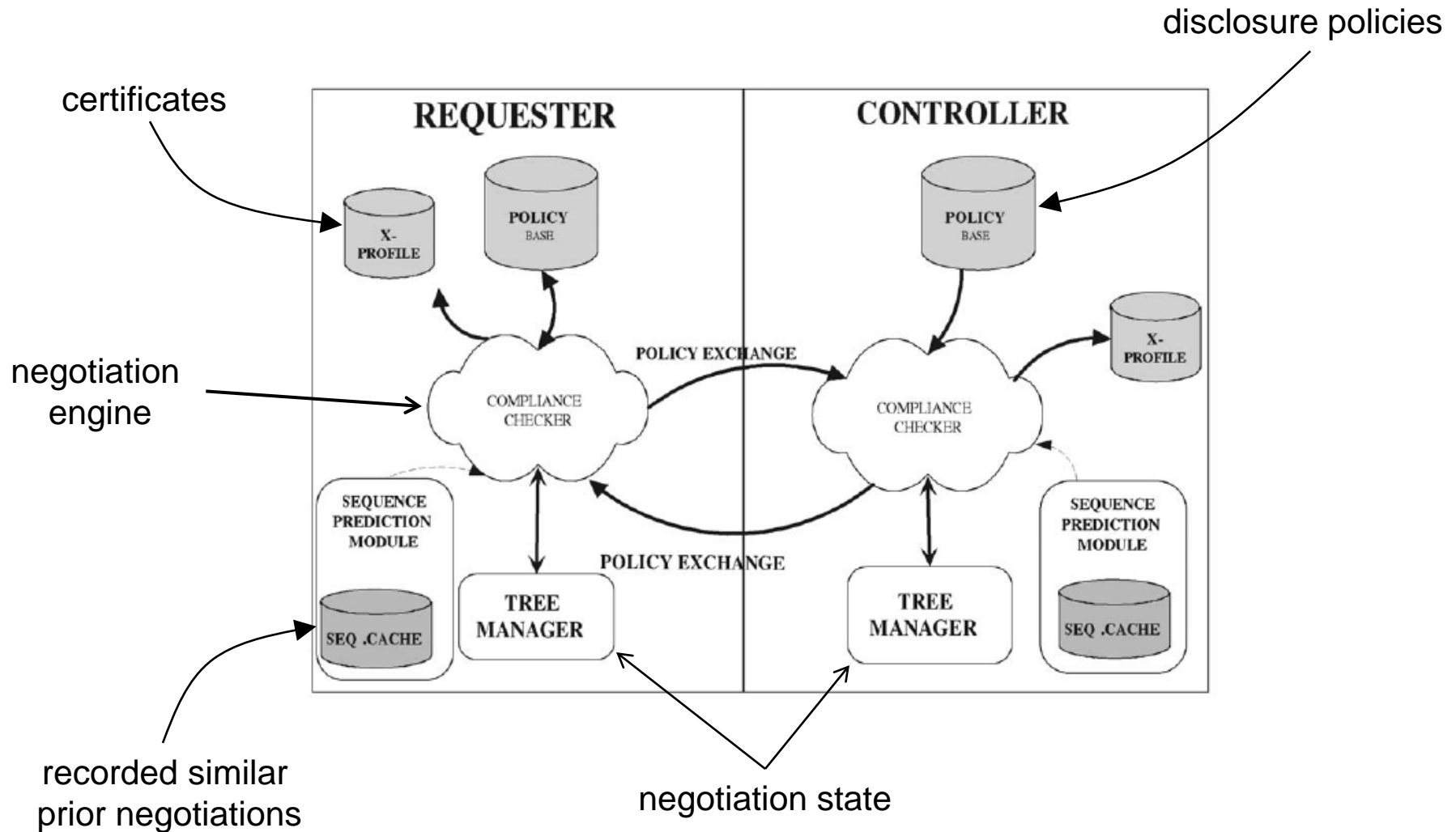
- Two remote interacting parties will disclose information to each other only when each has established an appropriate level of trust in the other.
- Elements
 - Remote peers
 - Requester (of a controlled resource)
 - Controller (of a requested resource)
 - Sensitive Information
 - data/services requested by remote peer
 - certificates
 - credentials: issued by trusted third party (e.g, affiliation)
 - declarations: attributes describing peer (e.g., preferences)
 - Negotiation
 - bilateral, incremental exchange leading to an authorization decision
 - Policies
 - drives exchange sequence
 - establish requirements for the disclosure of resources
 - alternative policies may exist for the same resource

Negotiation Overview

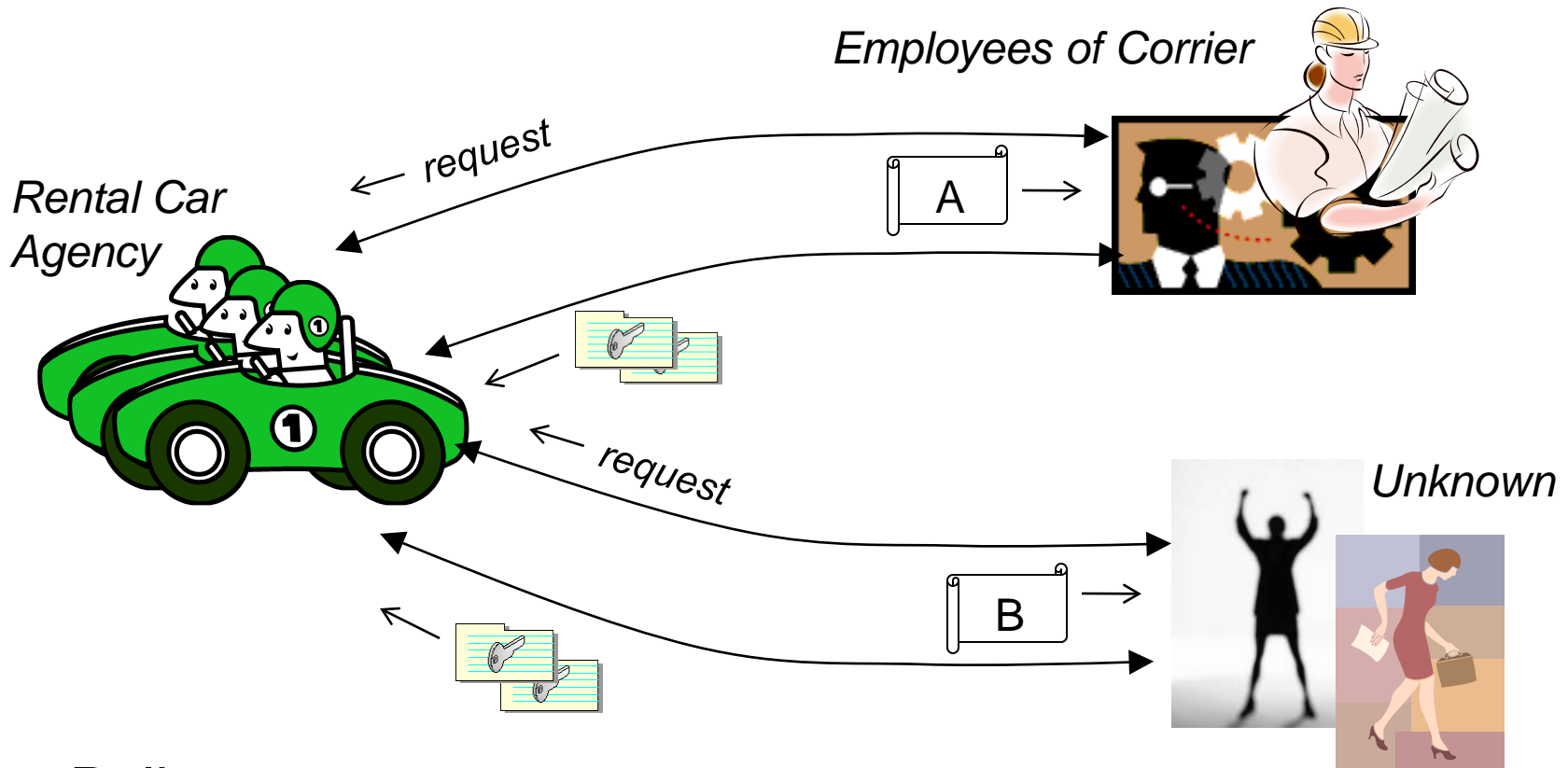


Slide modified from: <http://www.ccs.neu.edu/home/ahchan/wsl/symposium/bertino.ppt>

Trust-X Framework



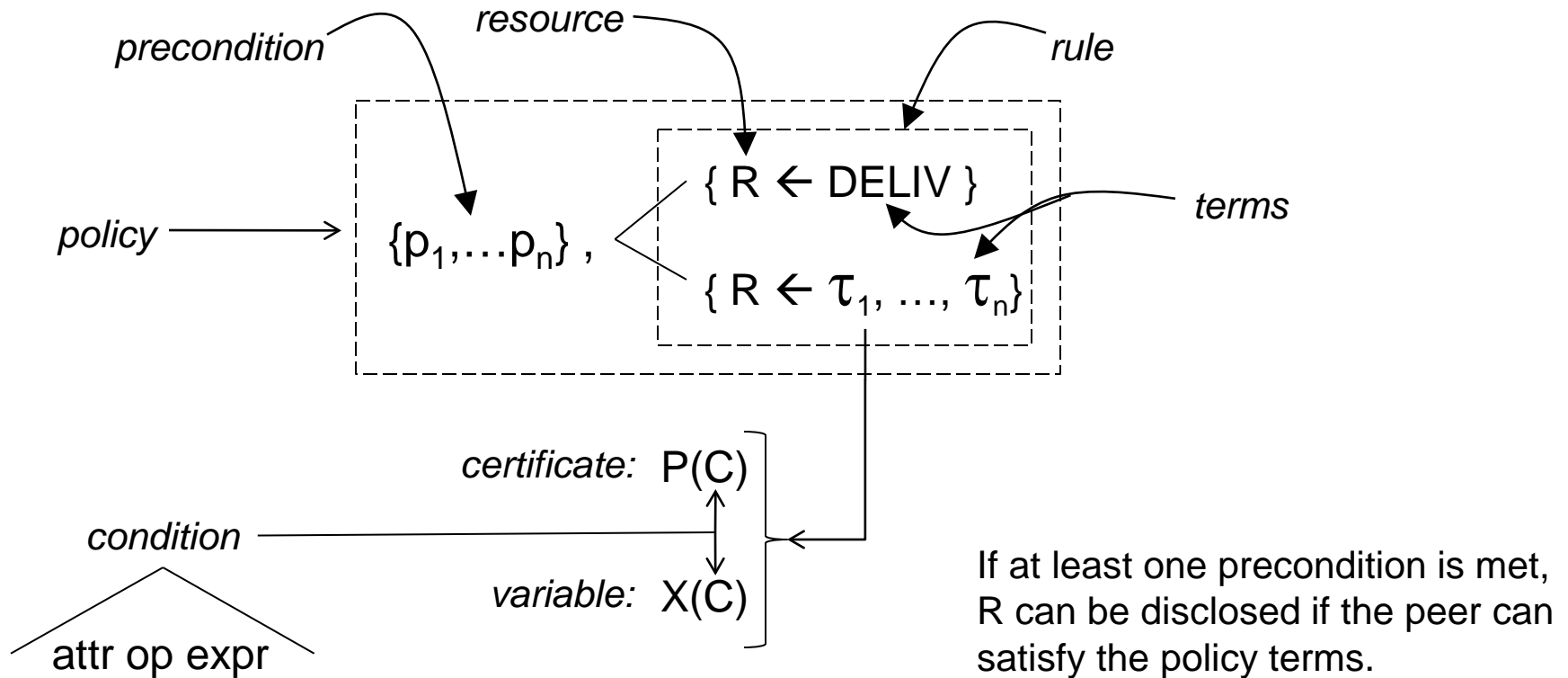
Scenario



Policy

- (A) Employees of Carrier must provide company badge and ID card
- (B) Others must provide drivers license and credit card

Disclosure Policy



$pol_3 = (\{pol_2\} , Rental_Car \leftarrow Credit_Card(name=Rental_Car.name, Rental_Car.ReturnDate < ExpirationDate));$

Policy for Scenario

$$pol_1 = (\{\}, Rental_Car \leftarrow Corrier_Employee$$

$$(code = Rental_Car.requesterCode,$$

$$position = driver), Id_Card$$

$$(name = Corrier_Employee.name));$$

$$pol_2 = (\{\}, Rental_Car \leftarrow Driving_Licence$$

$$(name = Rental_Car.name, issuer = EU));$$

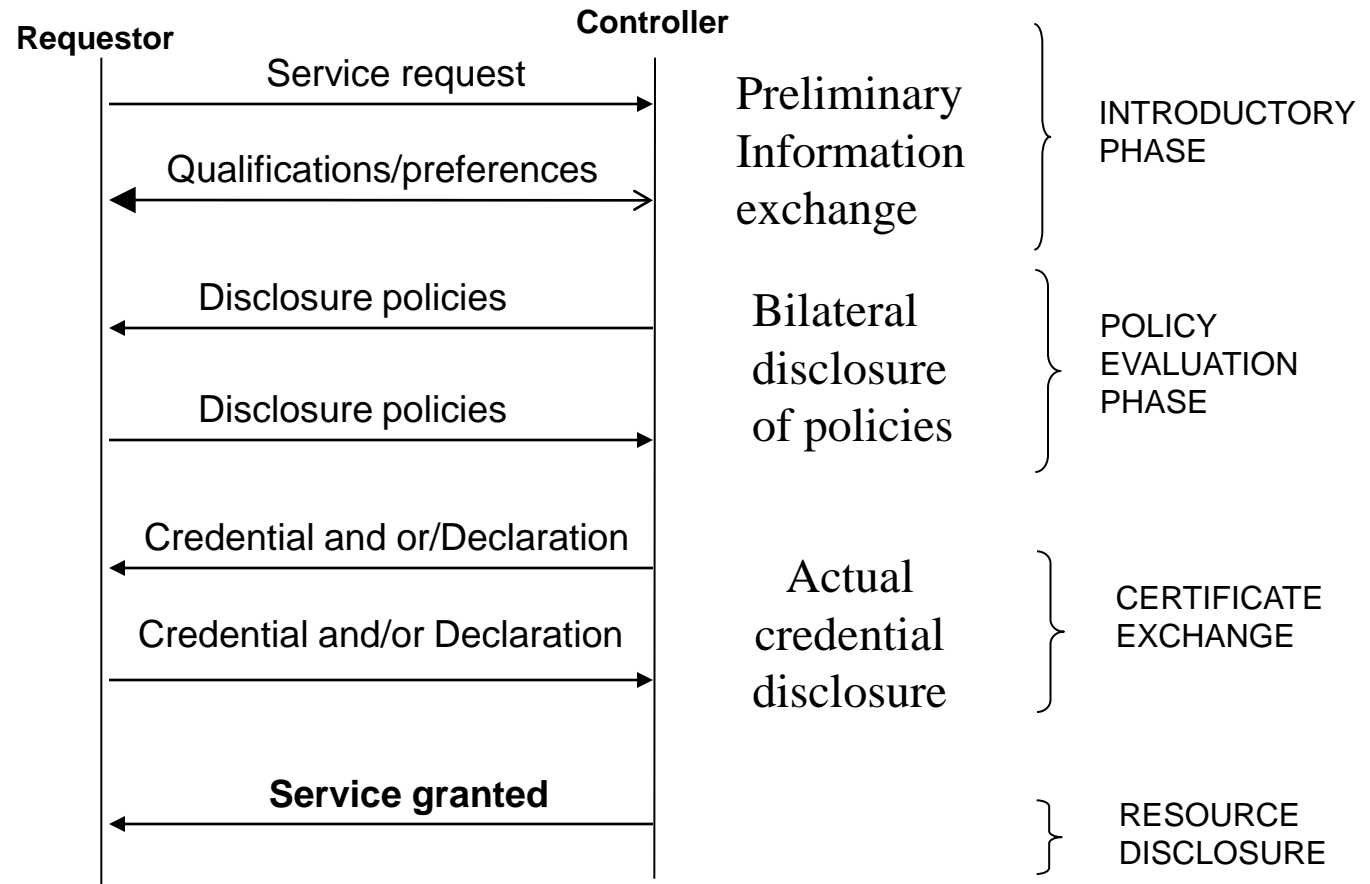
$$pol_3 = (\{pol_2\}, Rental_Car \leftarrow Credit_Card$$

$$(name = Rental_Car.nameRental_Car.ReturnDate$$

$$< ExpirationDate));$$

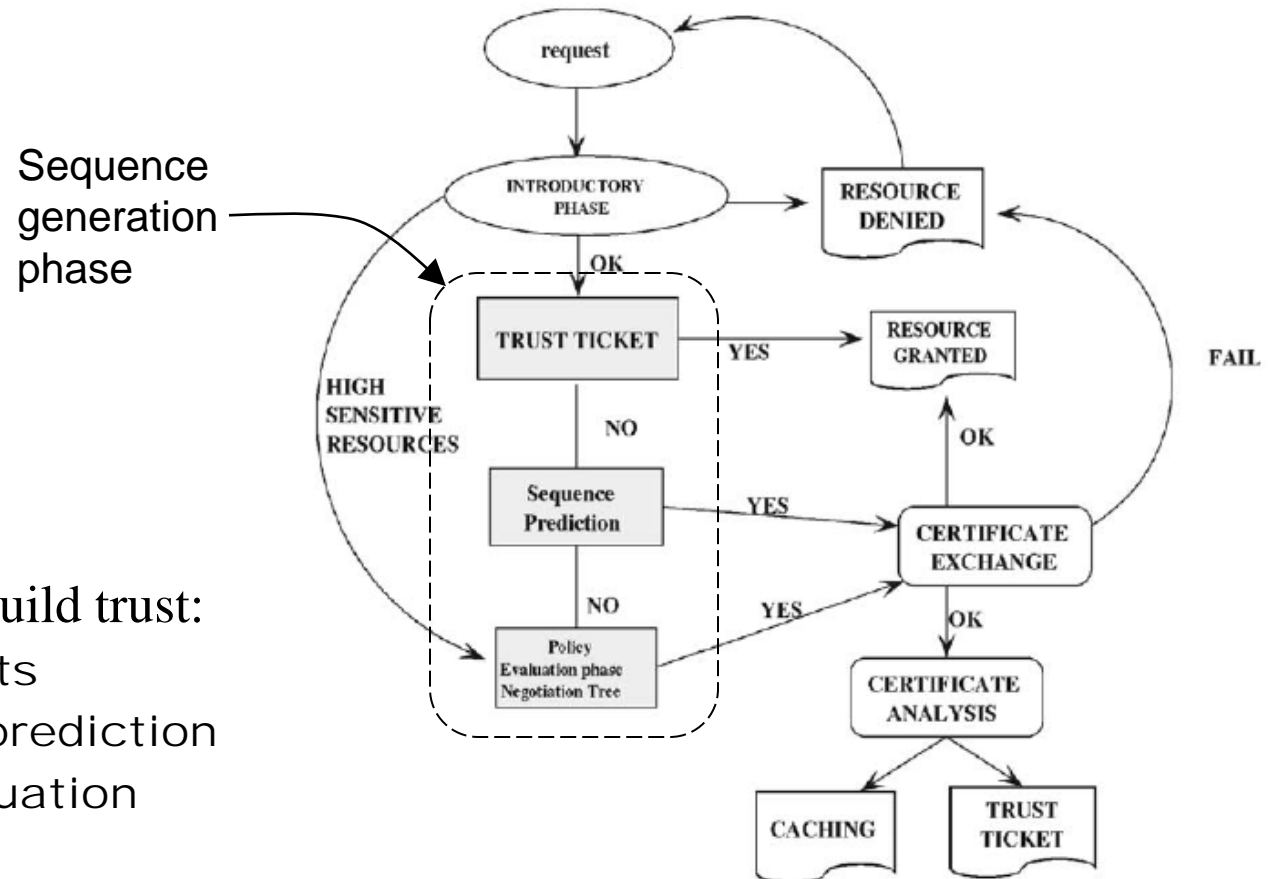
$$pol_4 = (\{pol_3, pol_1\}, Rental_Car \leftarrow DELIV).$$

Negotiation Process



Slide modified from: <http://www.ccs.neu.edu/home/ahchan/wsl/symposium/bertino.ppt>

Negotiation Process



- Three ways to build trust:
 1. Trust tickets
 2. Sequence prediction
 3. Policy evaluation

1. Trust Ticket

- Allows for expedited processing of repeat(ed) requests
- Certifies that parties have already successfully completed a negotiation for a given resource
- Issued by each party to the other at the end of a successful negotiation for access to that
- Reused for subsequent request for that resource
- Elements
 - Sequence of certificates
 - Validity time
 - Signature of issuer

2. Sequence Generation

- At the end of a successful negotiation for access to resource R, information about the sequence of peer credentials involved in the negotiation can be cached
- In a subsequent negotiation for resource R, the cached sequence can be retrieved and tested for applicability
- Useful in cases of repeated forms of negotiation with different parties

3. Policy Evaluation






■ Process

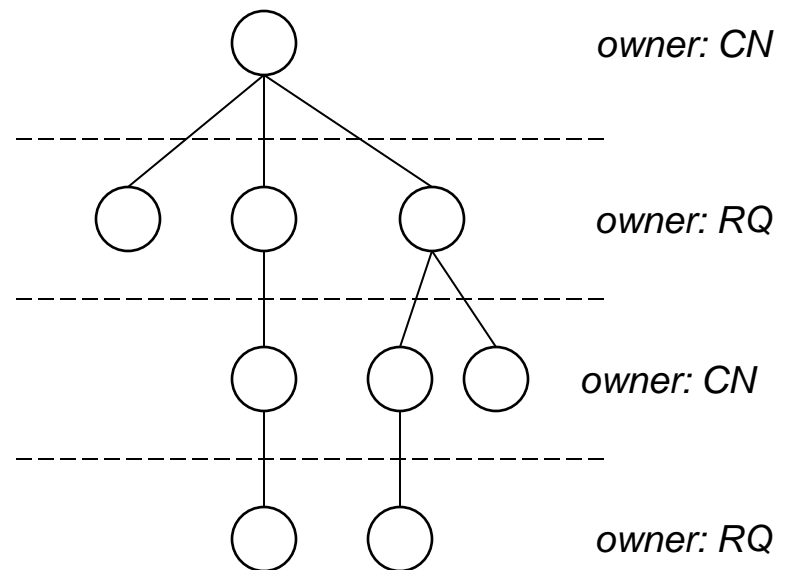
- Incremental exchange of policies driven by the resources each party requires of the other
- No credentials are exchanged during this phase
- Begins with initial request for access to resource
- Ends when
 - One party determines it cannot satisfy the policies of the other, or
 - Both parties believe/claim that they can each satisfy the other's policies

■ Elements

- Negotiation tree - maintains the state of the negotiation
- Labels - determine subsequent credential exchange order
- Views
 - path through the negotiation tree
 - trust sequence: a view where all policies are satisfied

Negotiation Tree

GRAPH NOTATION	MEANING
	open node
	simple edge
	multi edge
	deliv node
	linked nodes

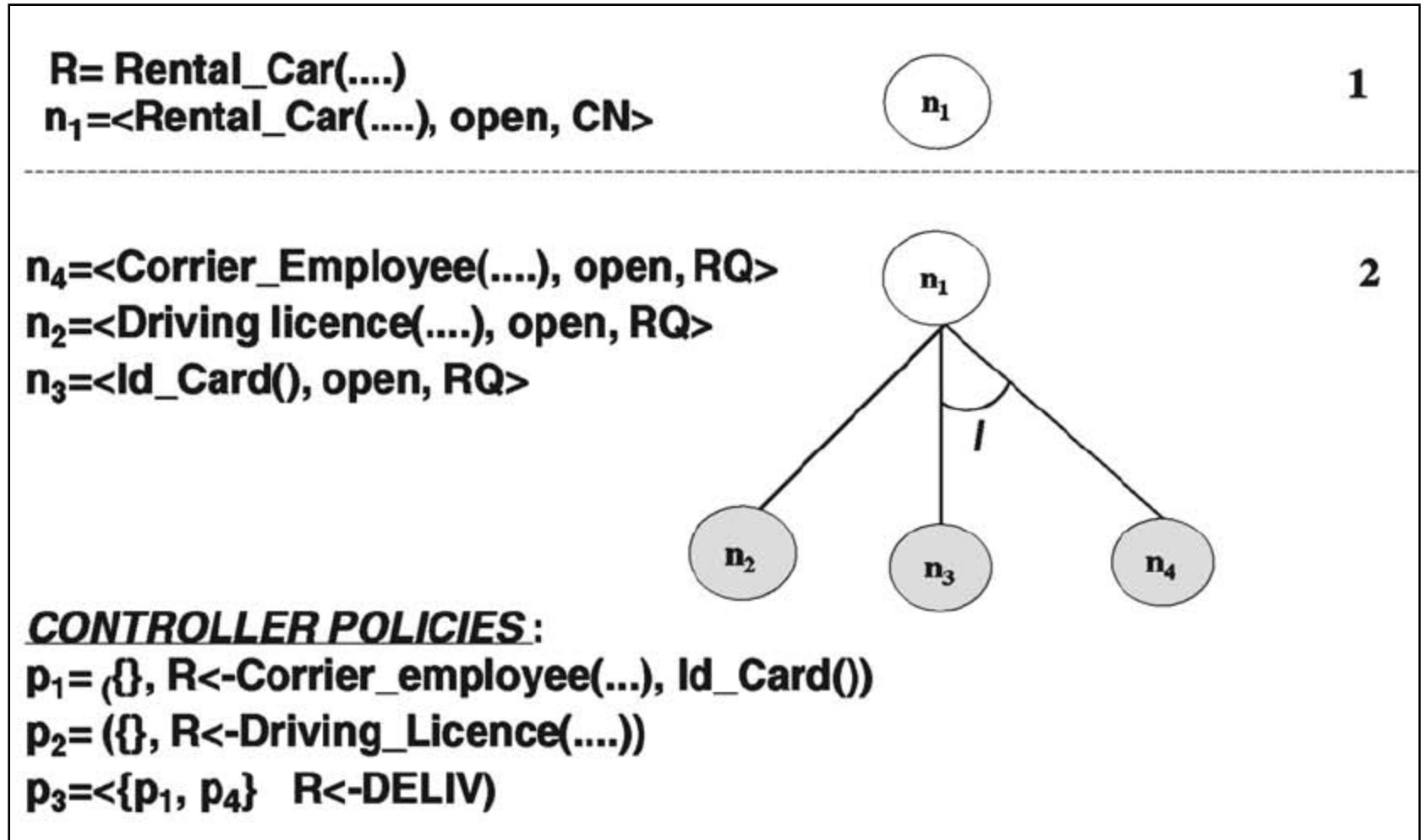


node: <resource, state, owner>

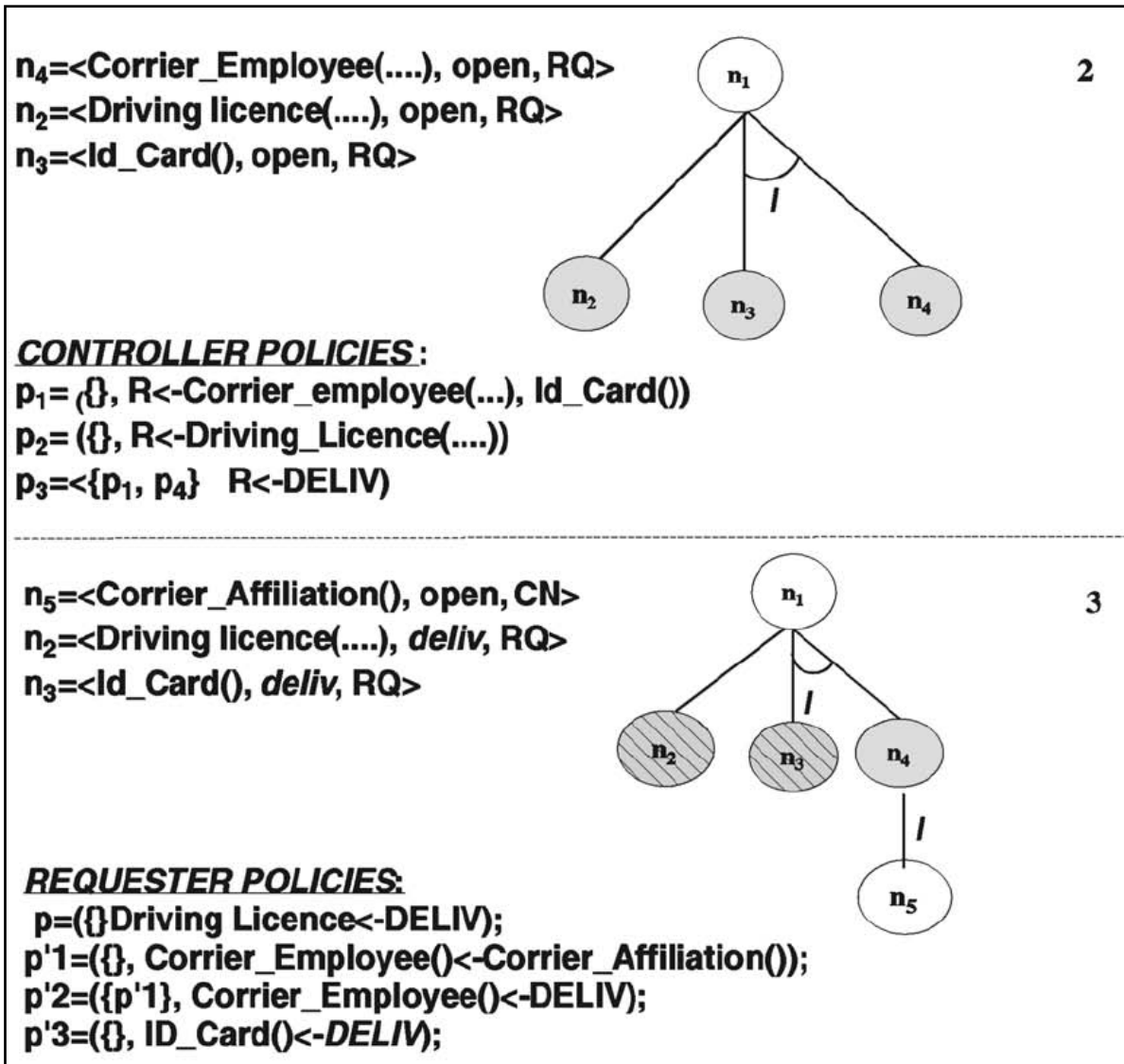
state: open or DELIV

owner: RQ (requestor), CN (controller)

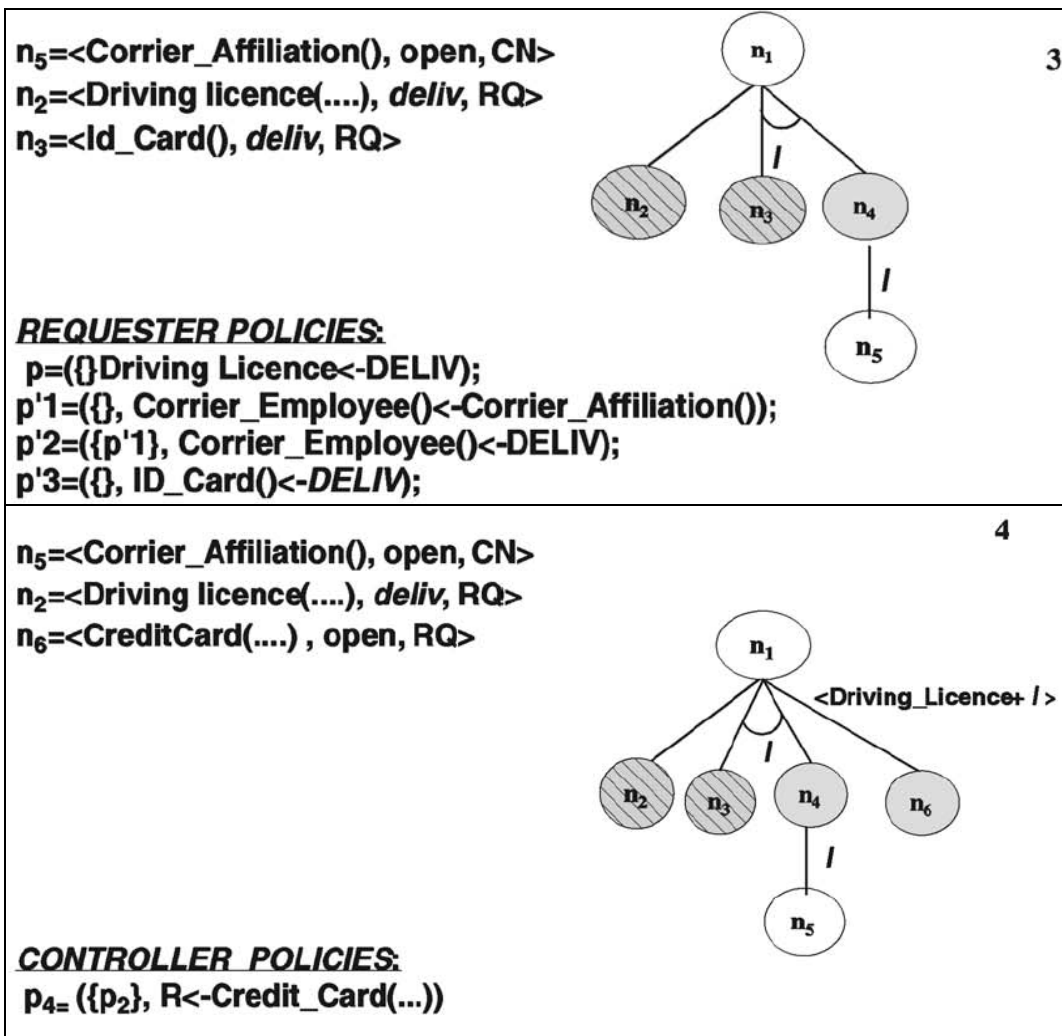
Example Negotiation Tree



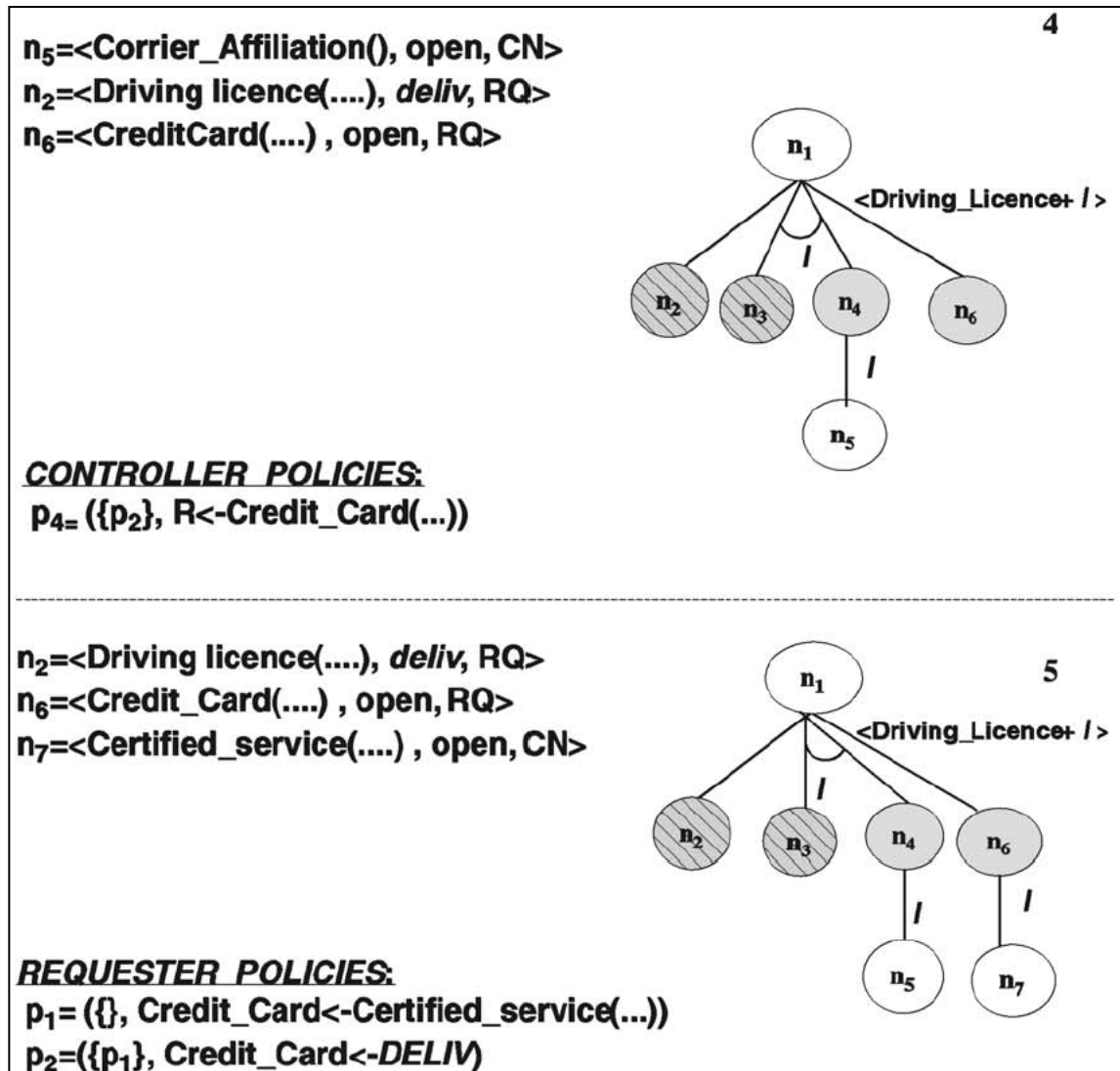
Example Negotiation Tree



Example Negotiation Tree



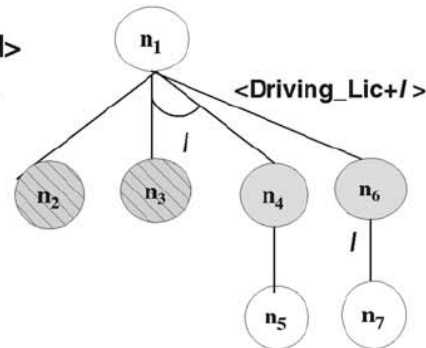
Example Negotiation Tree



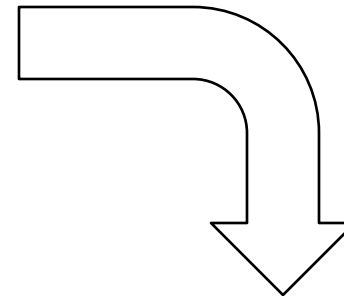
Example Negotiation Tree

$n_6 = \langle \text{CreditCard}(\dots), \text{open}, \text{RQ} \rangle$
 $n_7 = \langle \text{Certified_service}(\dots), \text{open}, \text{CN} \rangle$
 $n_5 = \langle \text{Carrier_Affiliation}(), \text{open}, \text{CN} \rangle$
 $n_2 = \langle \text{Driving licence}(\dots), \text{deliv}, \text{RQ} \rangle$
 $n_3 = \langle \text{Id_Card}(), \text{deliv}, \text{RQ} \rangle$

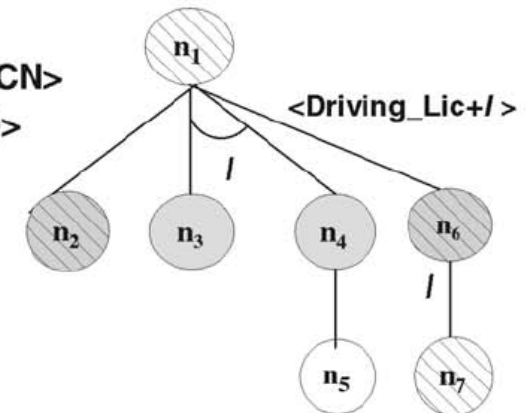
CONTROLLER POLICY:
 $p_4 = (\{\} \text{Certified_service} \leftarrow \text{DELIV})$



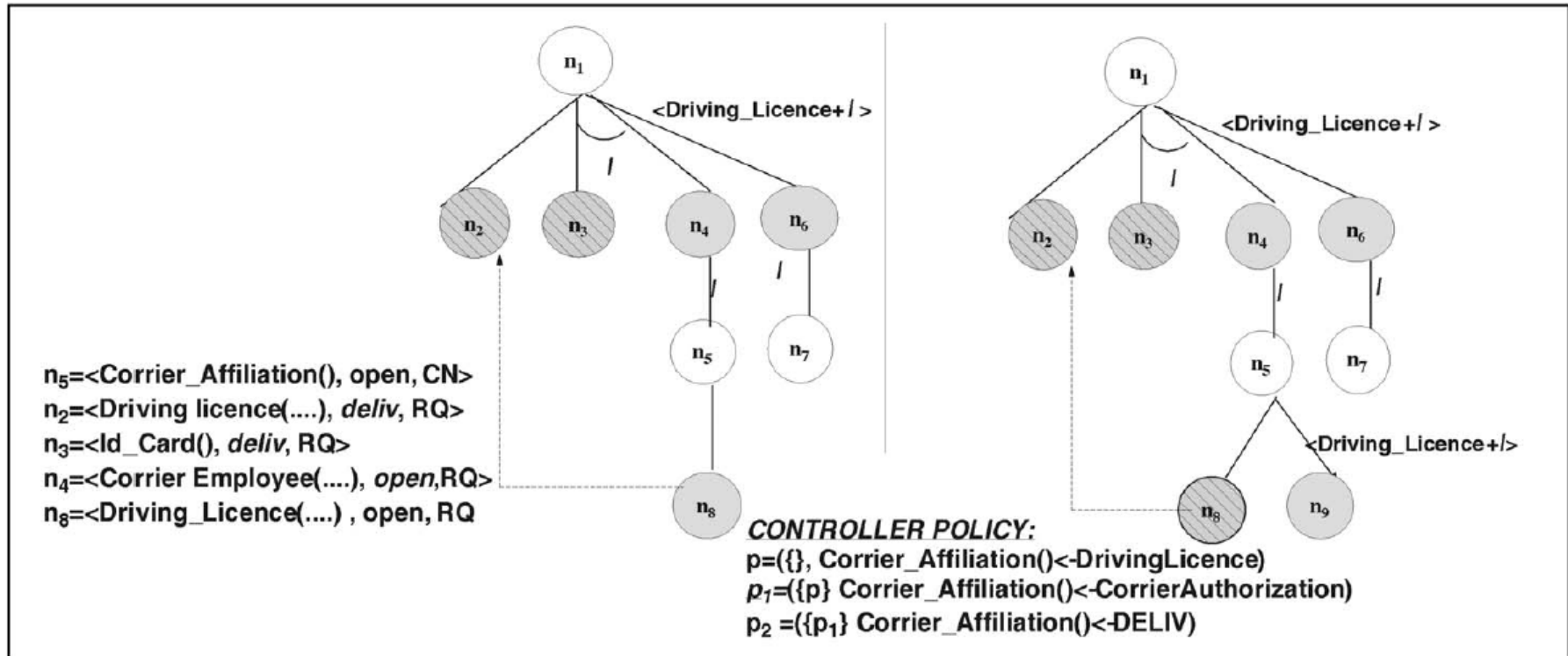
Assume that Certified_service is not controlled by any policy



$n_1 = \langle \text{Rental_Car}(), \text{deliv}, \text{CN} \rangle$
 $n_6 = \langle \text{CreditCard}(\dots), \text{deliv}, \text{RQ} \rangle$
 $n_7 = \langle \text{Certified_service}(\dots), \text{deliv}, \text{CN} \rangle$
 $n_2 = \langle \text{Driving licence}(\dots), \text{deliv}, \text{RQ} \rangle$
 $n_3 = \langle \text{Id_Card}(), \text{deliv}, \text{RQ} \rangle$



Repeated Nodes



- link nodes referring to the same resource to avoid duplicating exchange/evaluation

Edge Labels

- When the precondition for a policy, P , is satisfied, nodes corresponding to P can be added to the negotiation tree
- The certificates satisfying the precondition policies are used to label the edges for the nodes corresponding to P
- The edge labels denote the order of credential exchange

