

Attribute-Based Access Control Models and Beyond

Prof. Ravi Sandhu

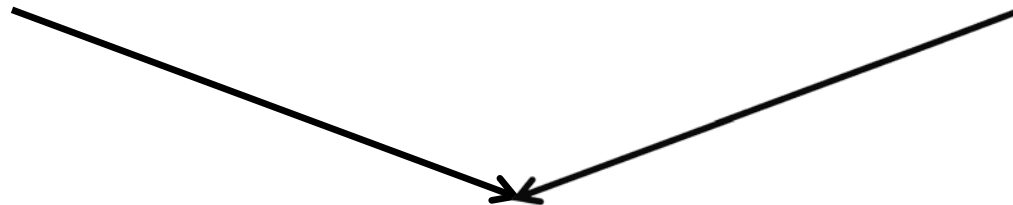
Executive Director, Institute for Cyber Security
Lutcher Brown Endowed Chair in Cyber Security
University of Texas at San Antonio

AsiaCCS Keynote Talk
Singapore
April 16, 2015

ravi.sandhu@utsa.edu, www.profsandhu.com, www.ics.utsa.edu

**Discretionary Access Control
(DAC), 1970**

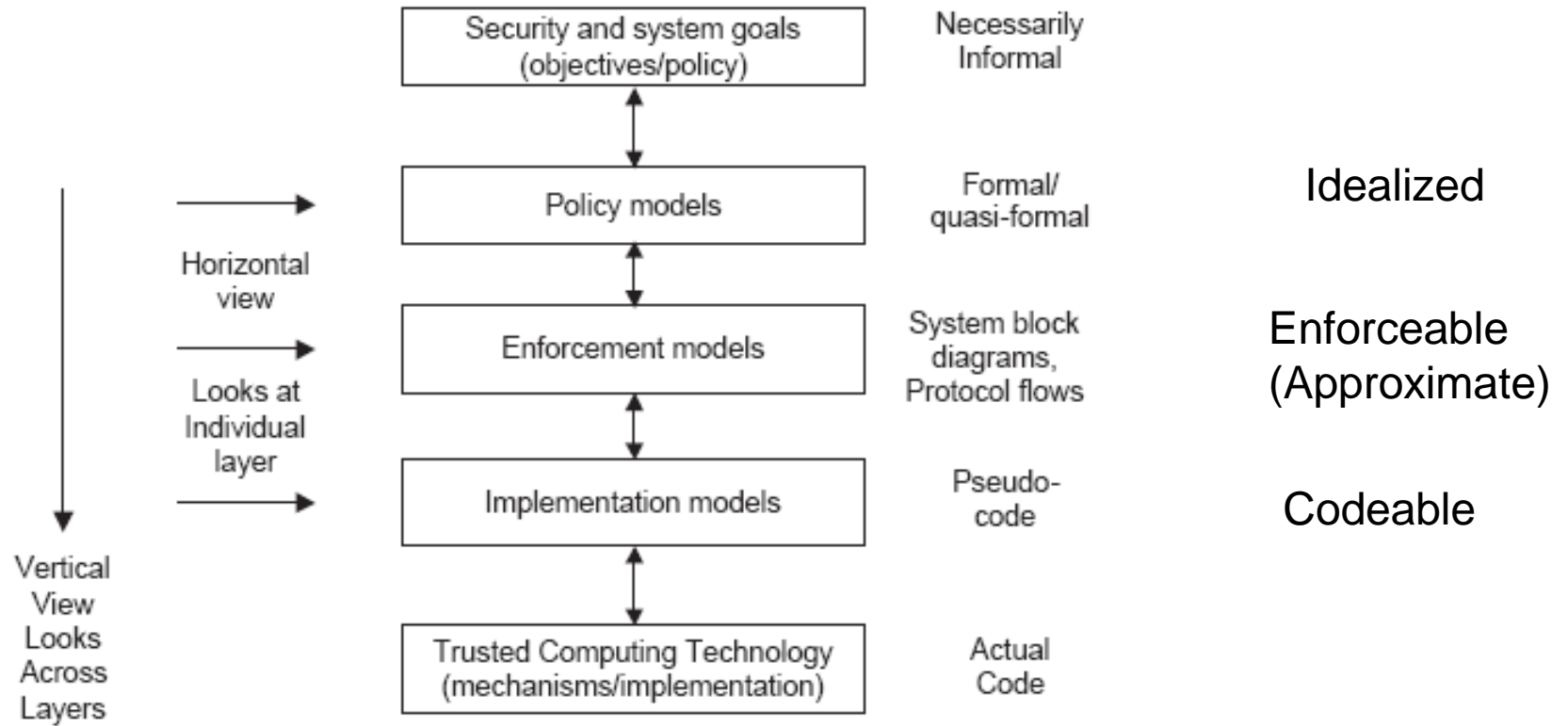
**Mandatory Access Control
(MAC), 1970**



**Role Based Access Control
(RBAC), 1995**

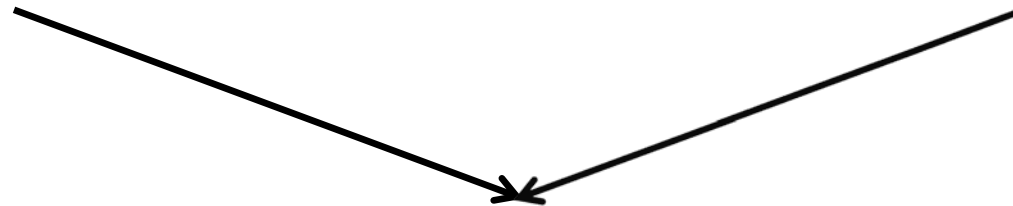


**Attribute Based Access Control
(ABAC), ????**



**Discretionary Access Control
(DAC), 1970**

**Mandatory Access Control
(MAC), 1970**



**Role Based Access Control
(RBAC), 1995**



**Attribute Based Access Control
(ABAC), ????**

**Fixed
policy**



**Discretionary Access Control
(DAC), 1970**

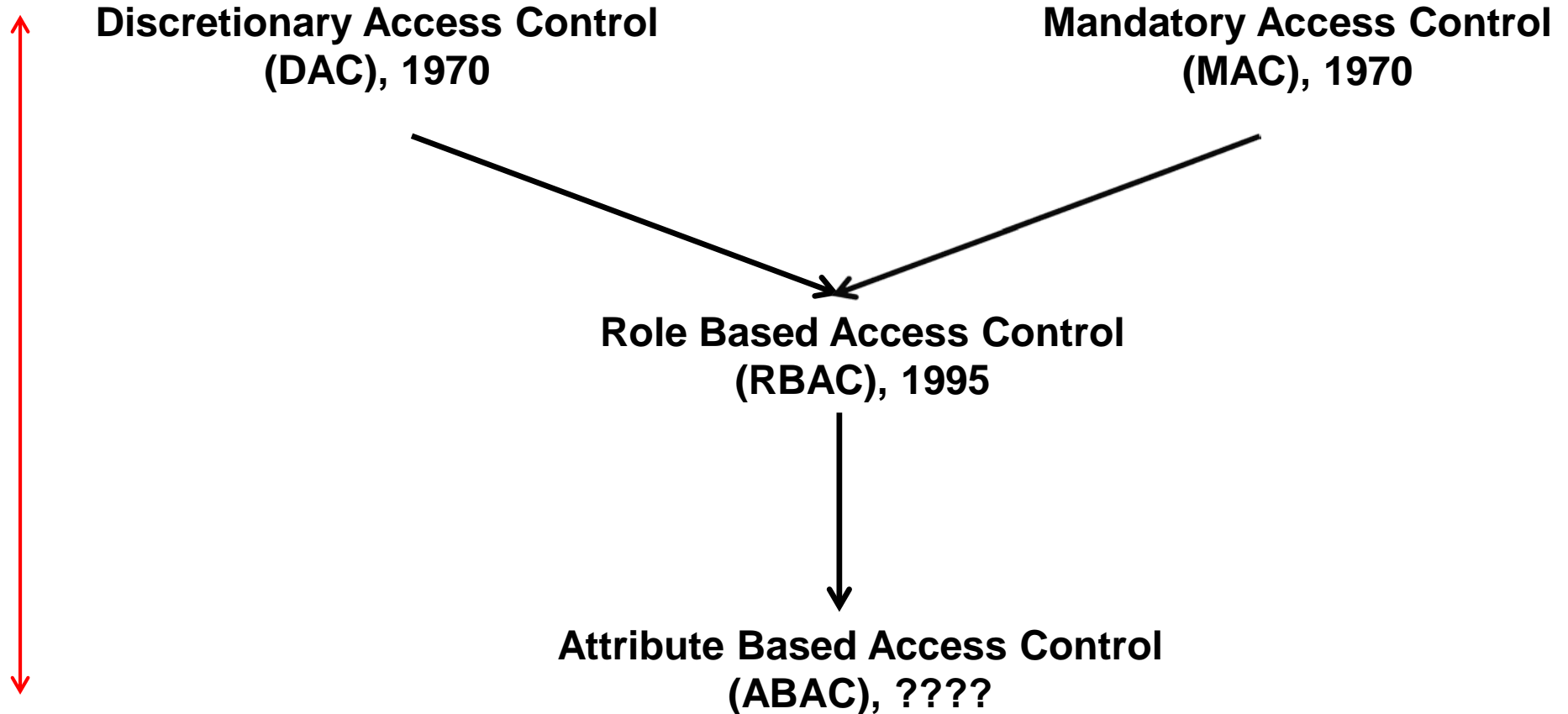
**Mandatory Access Control
(MAC), 1970**

**Role Based Access Control
(RBAC), 1995**

**Attribute Based Access Control
(ABAC), ????**

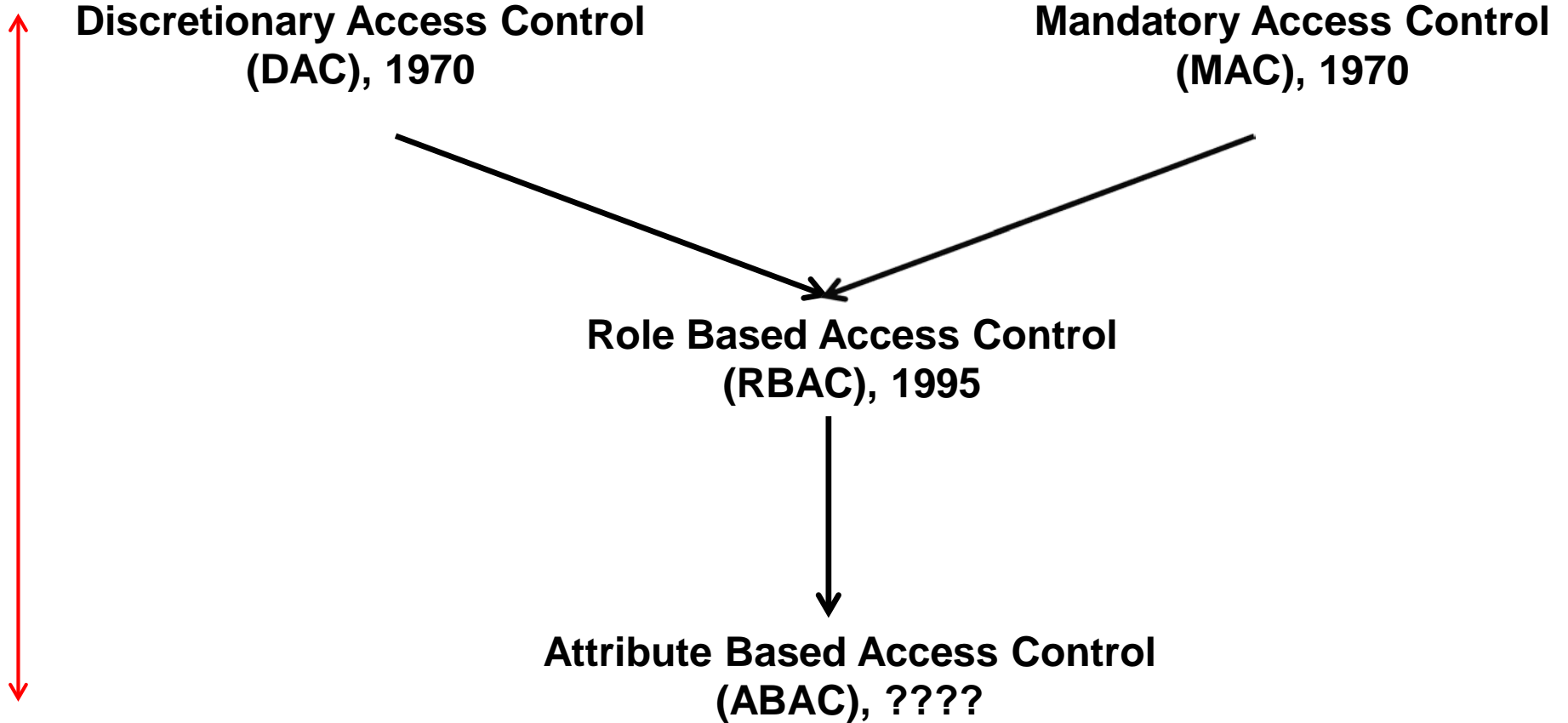
**Flexible
policy**

**Enterprise
Oriented**

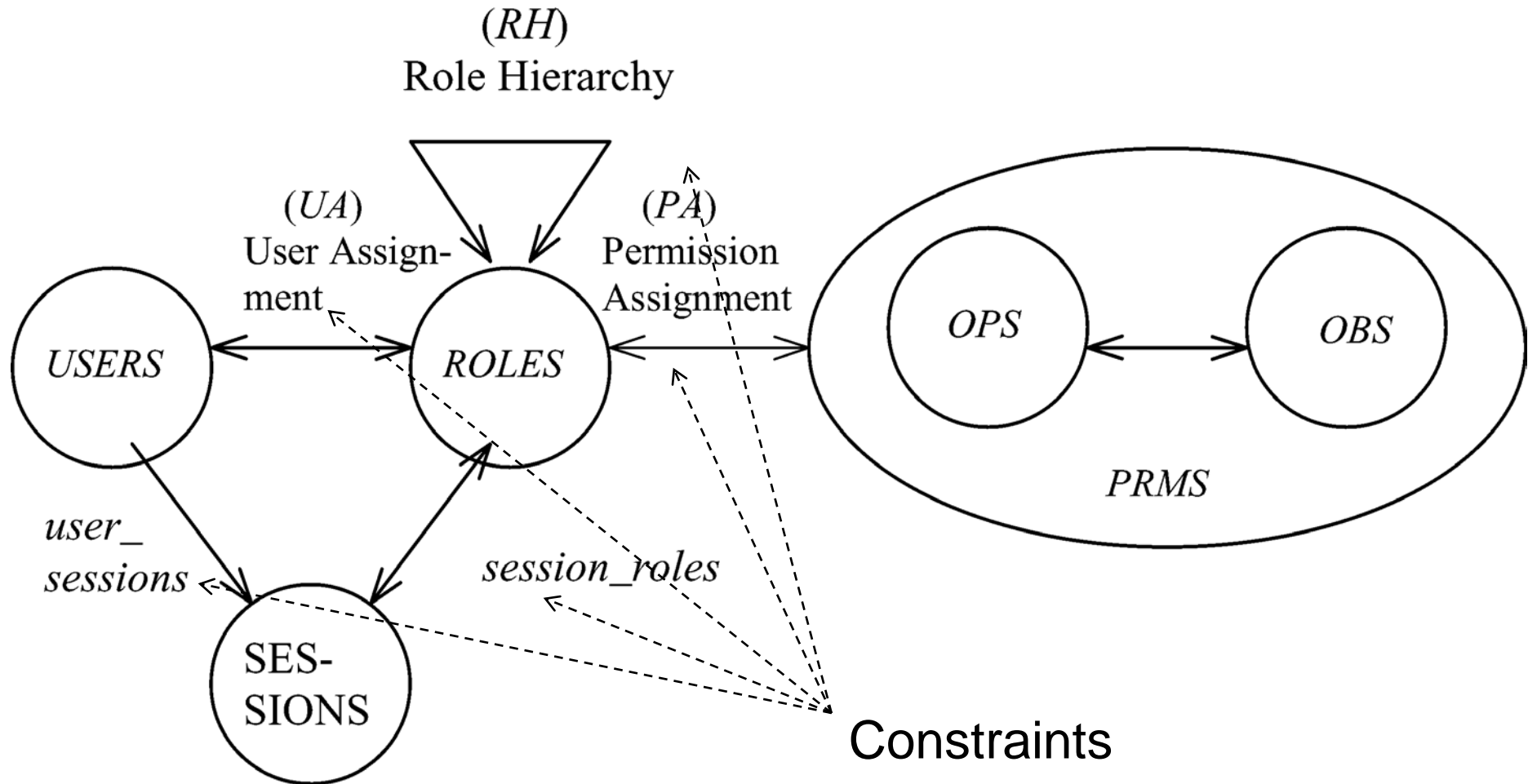


**Beyond
Enterprise**

**Administration
Driven**



**Automated
Adaptive**

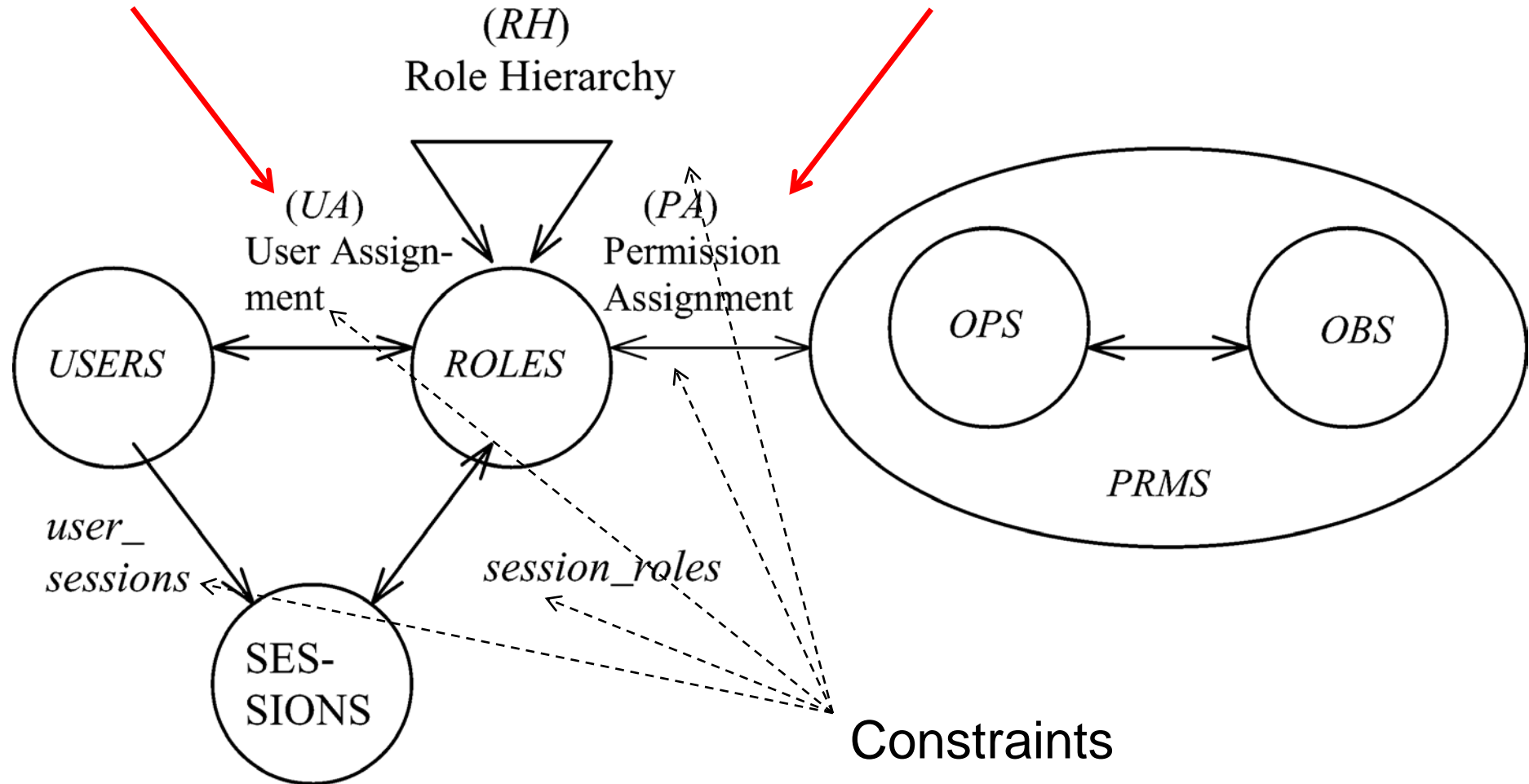


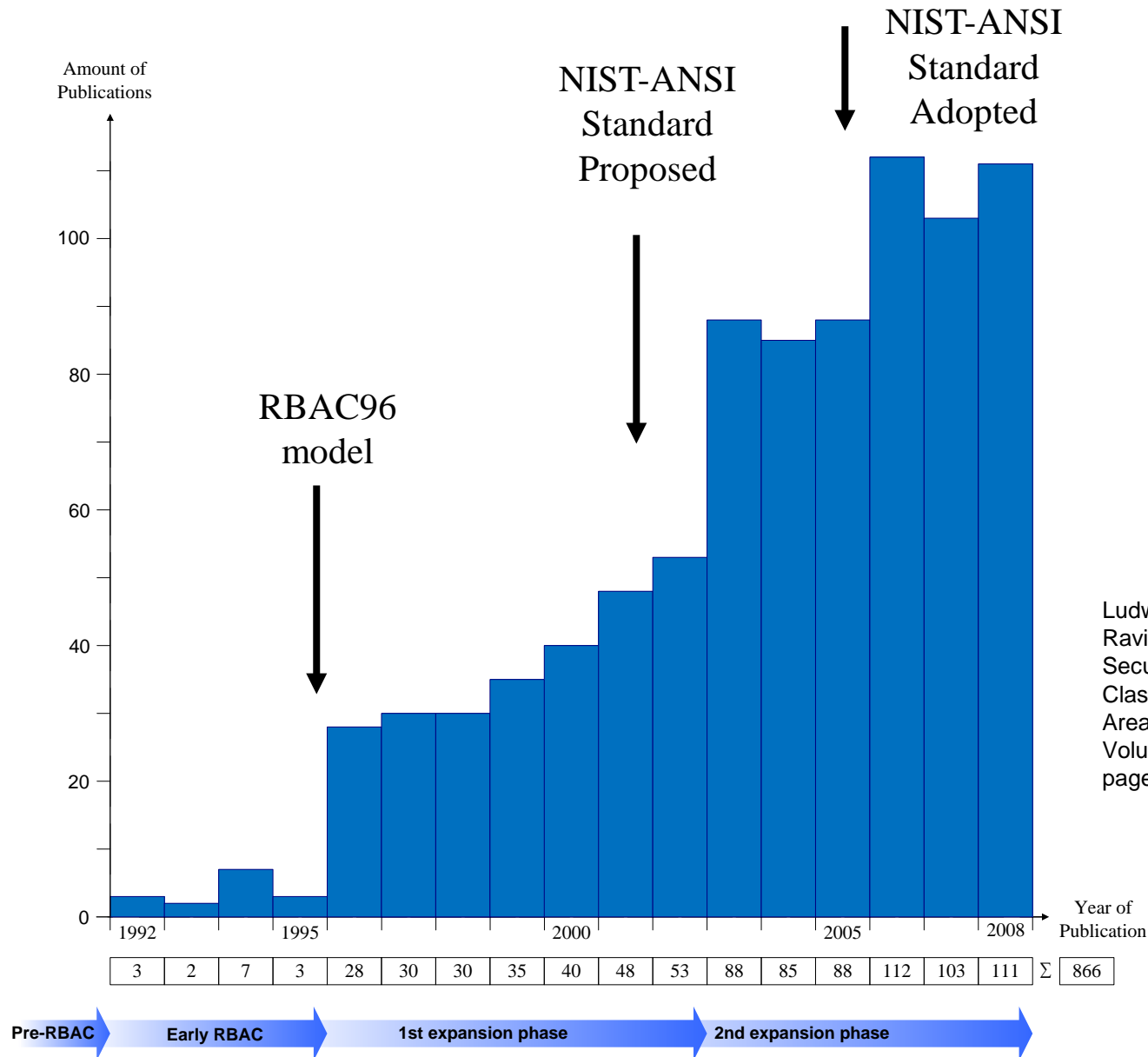
- RBAC can be configured to do MAC
- RBAC can be configured to do DAC
- RBAC is policy neutral

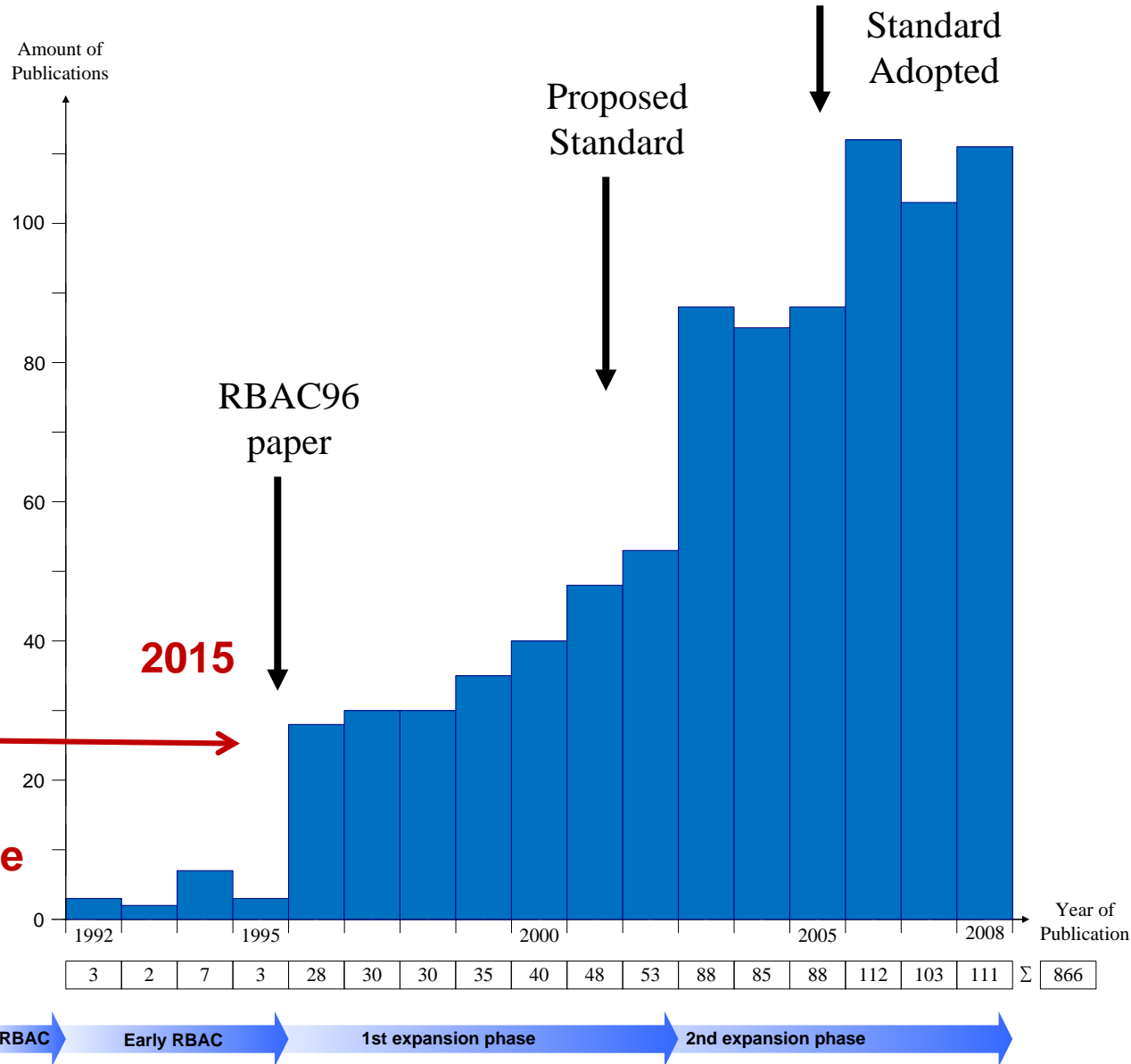
RBAC is neither MAC nor DAC!

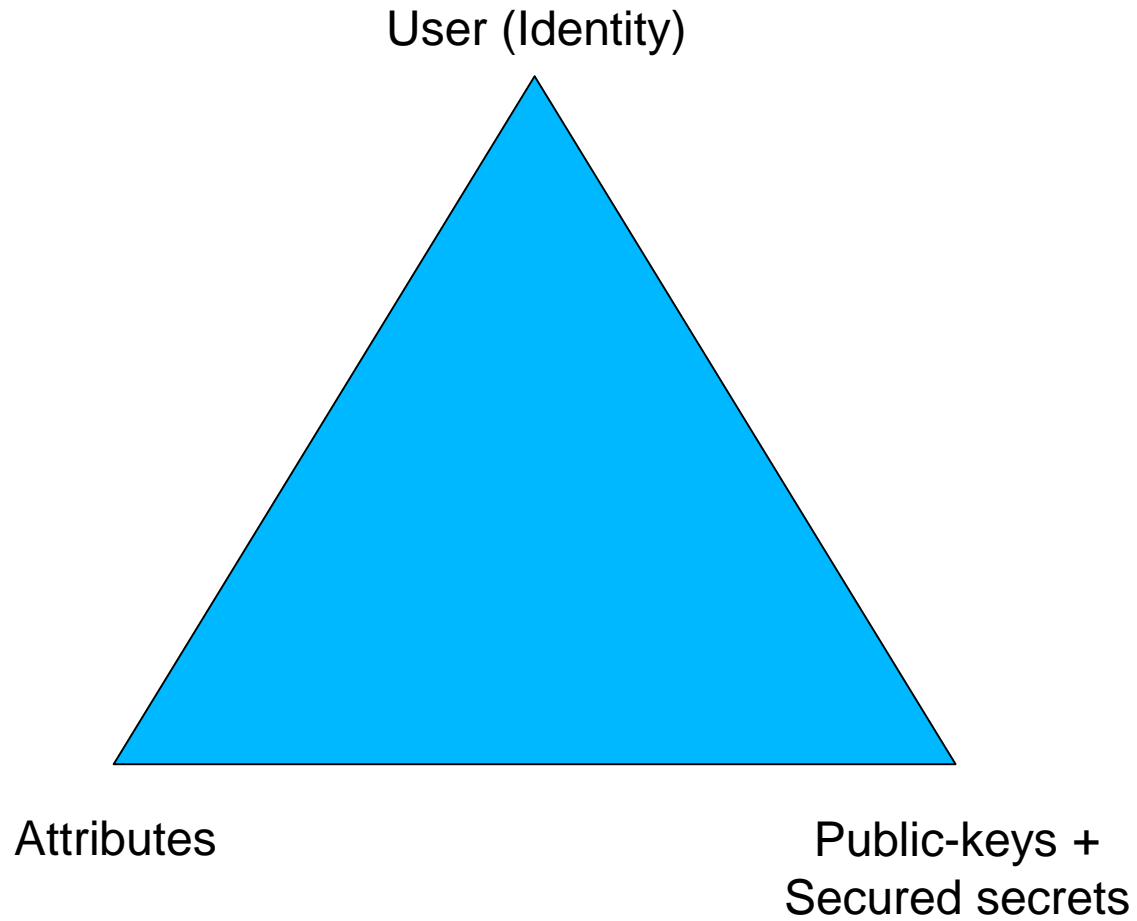
Hard Enough

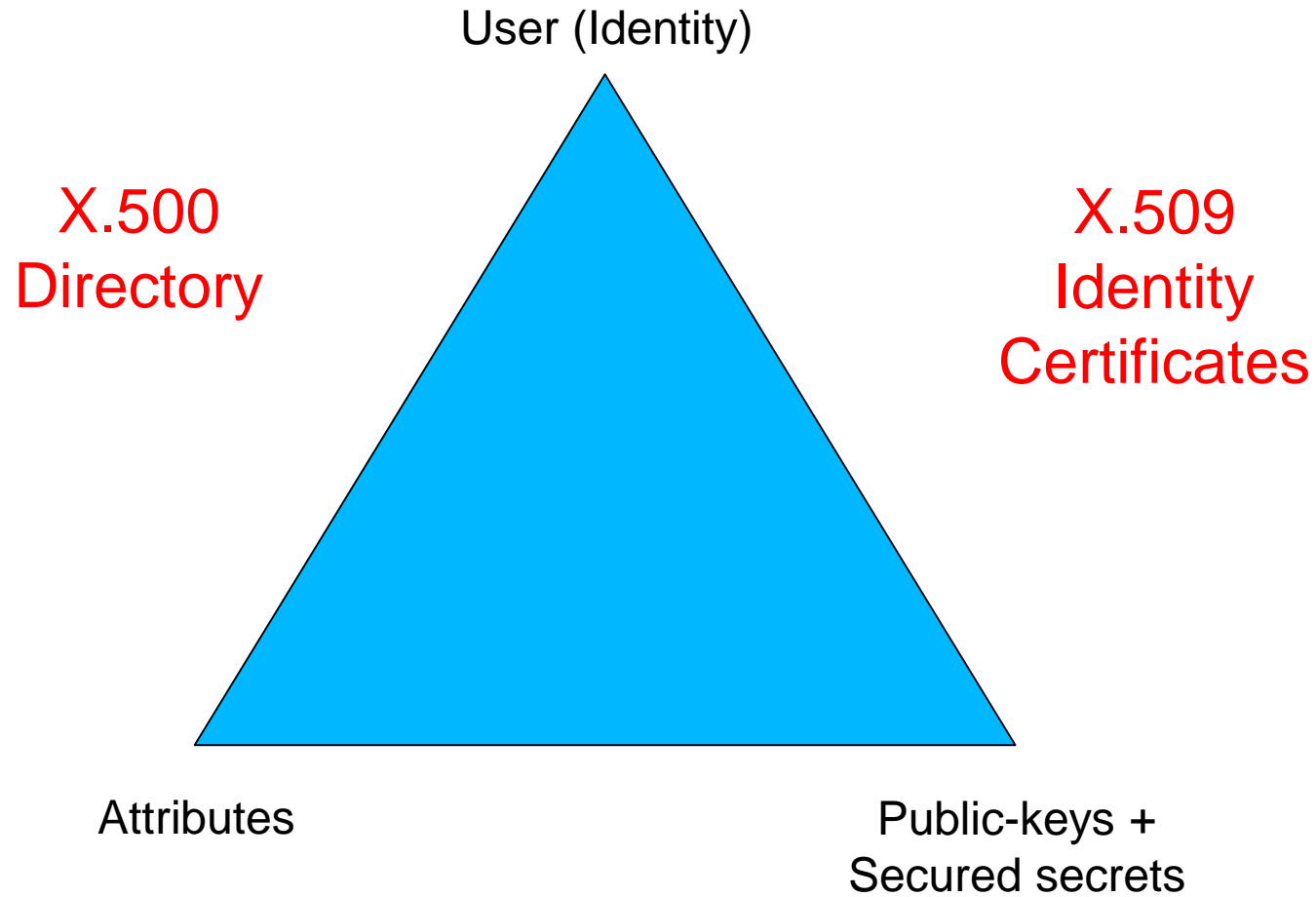
Impossible



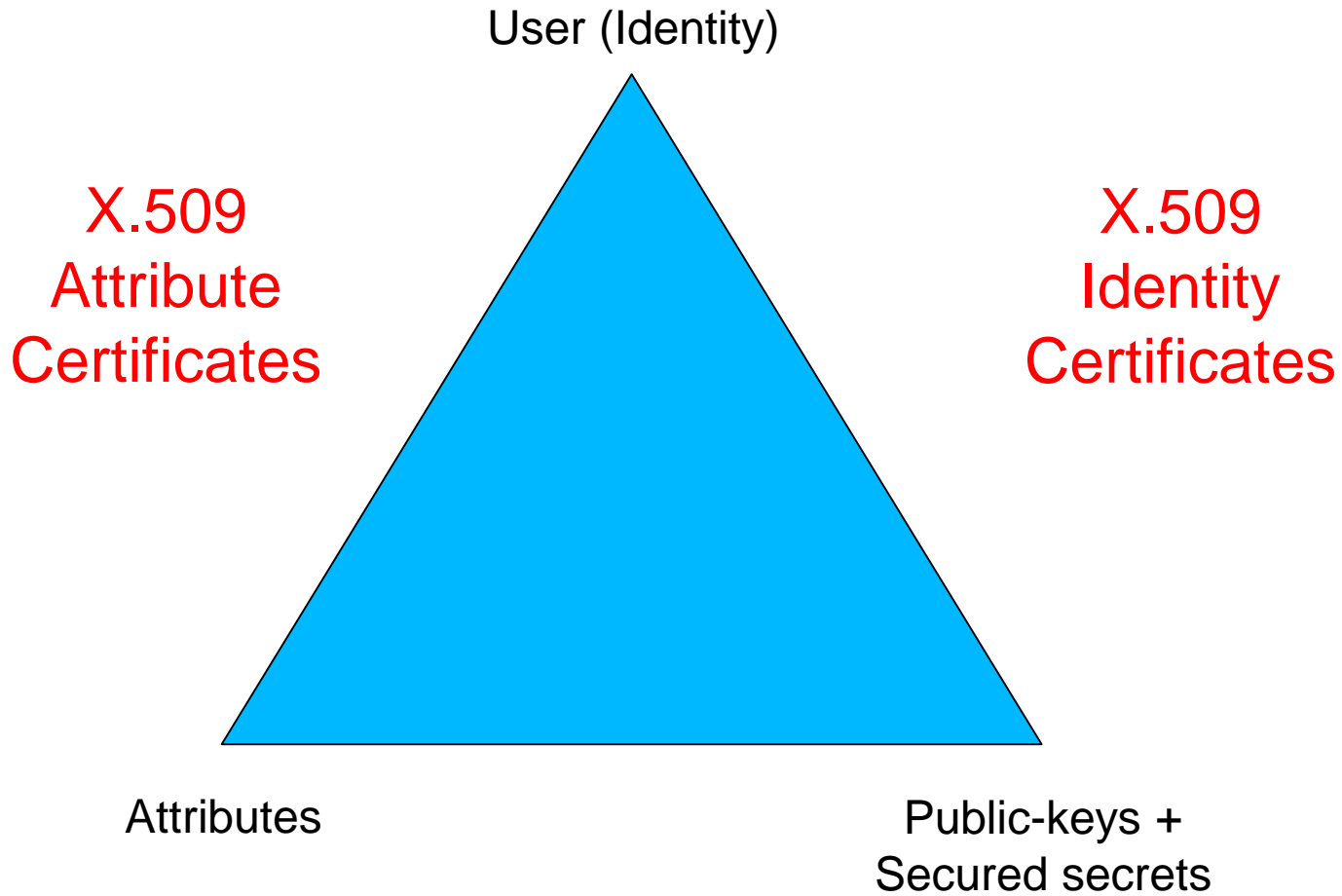




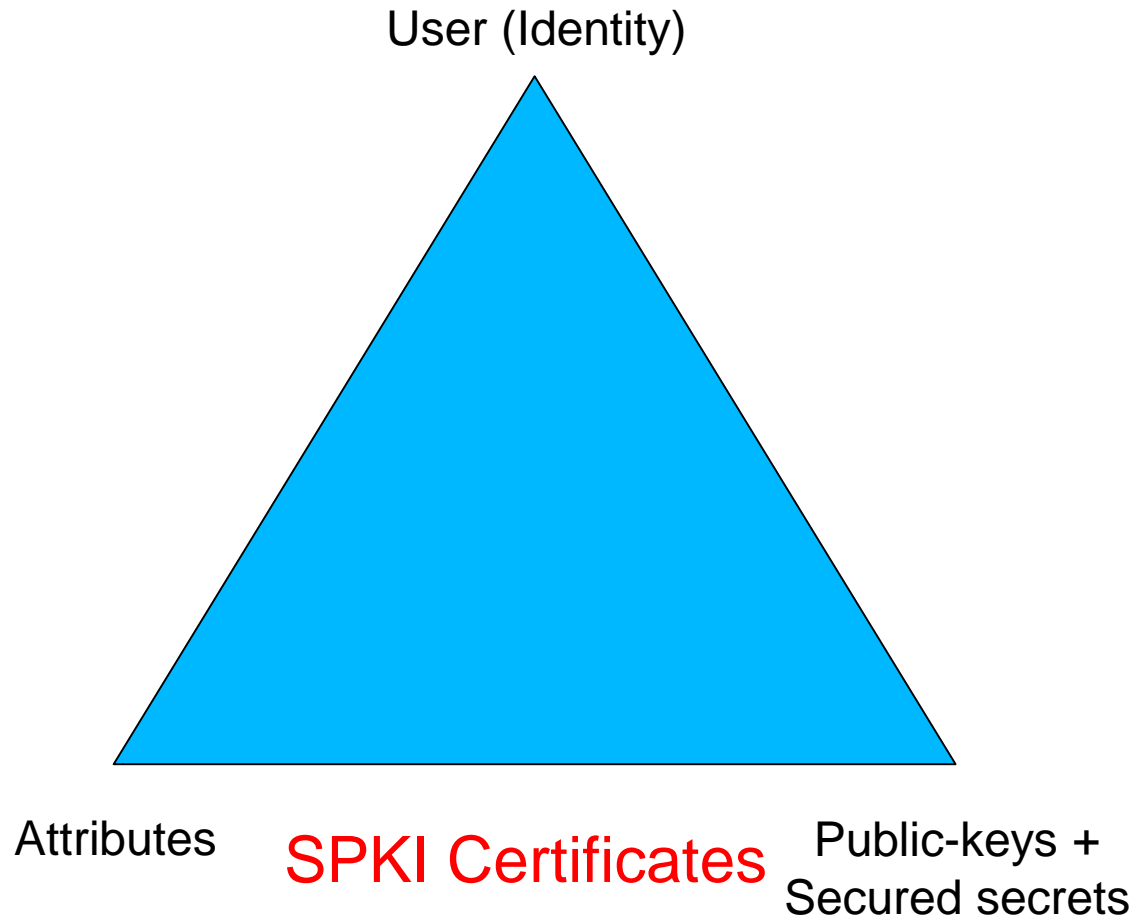




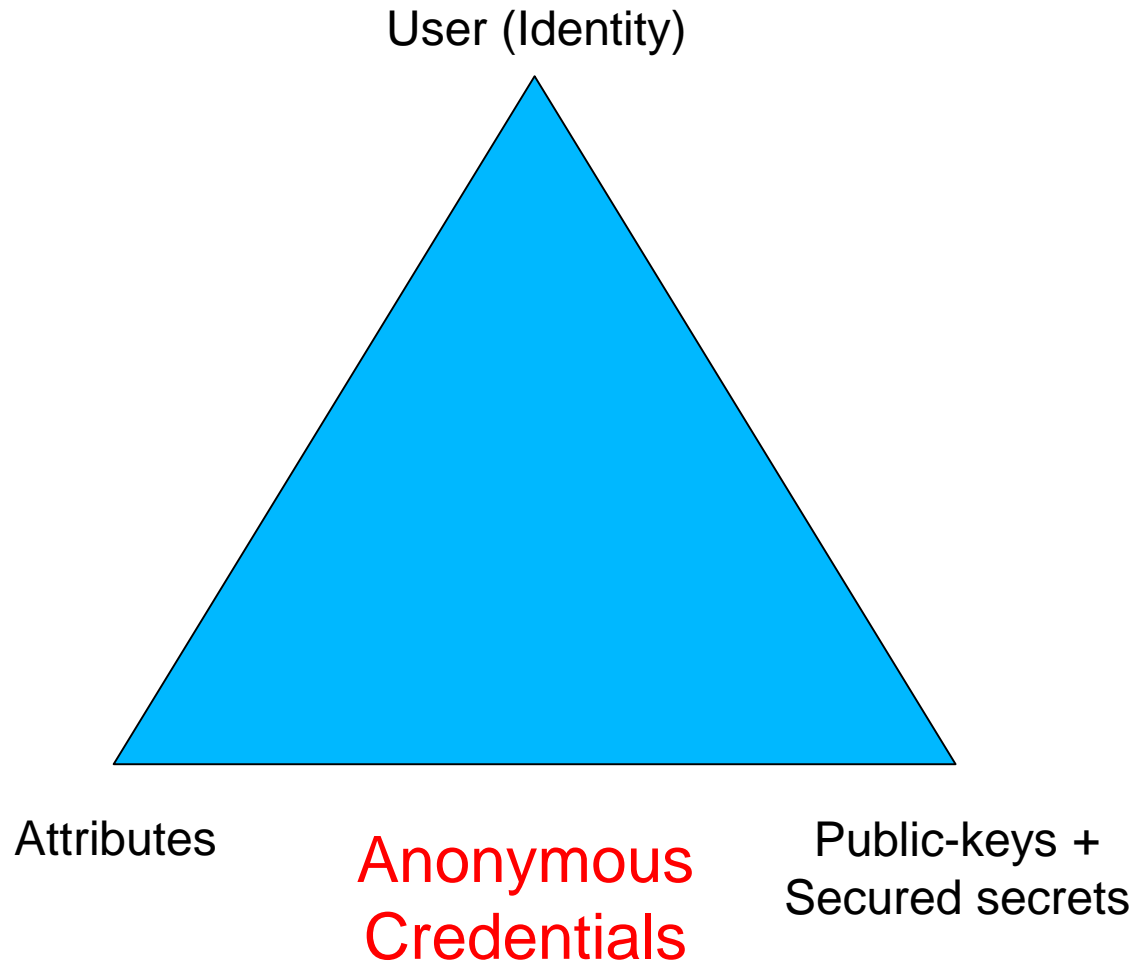
Pre Internet, early 1990s



Post Internet, late 1990s

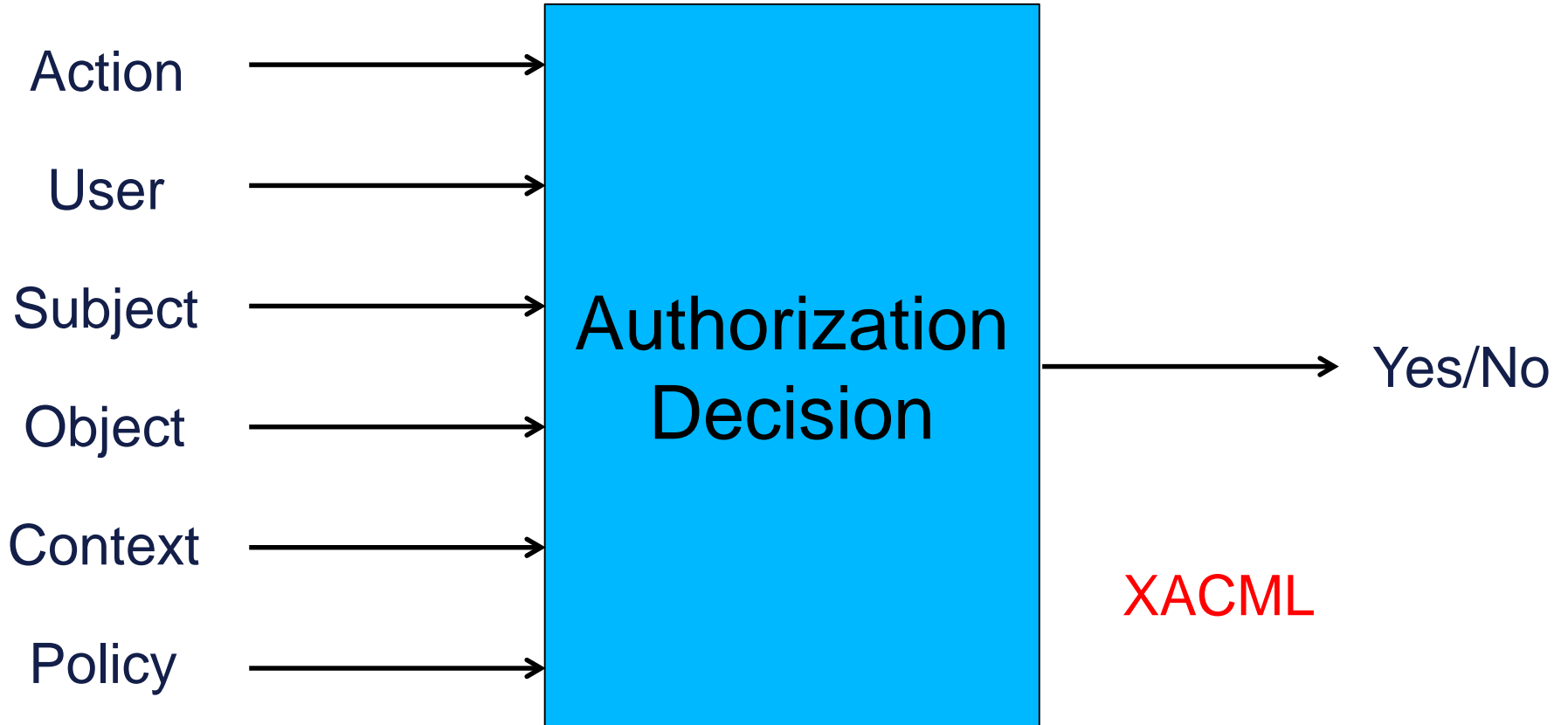


Post Internet, late 1990s



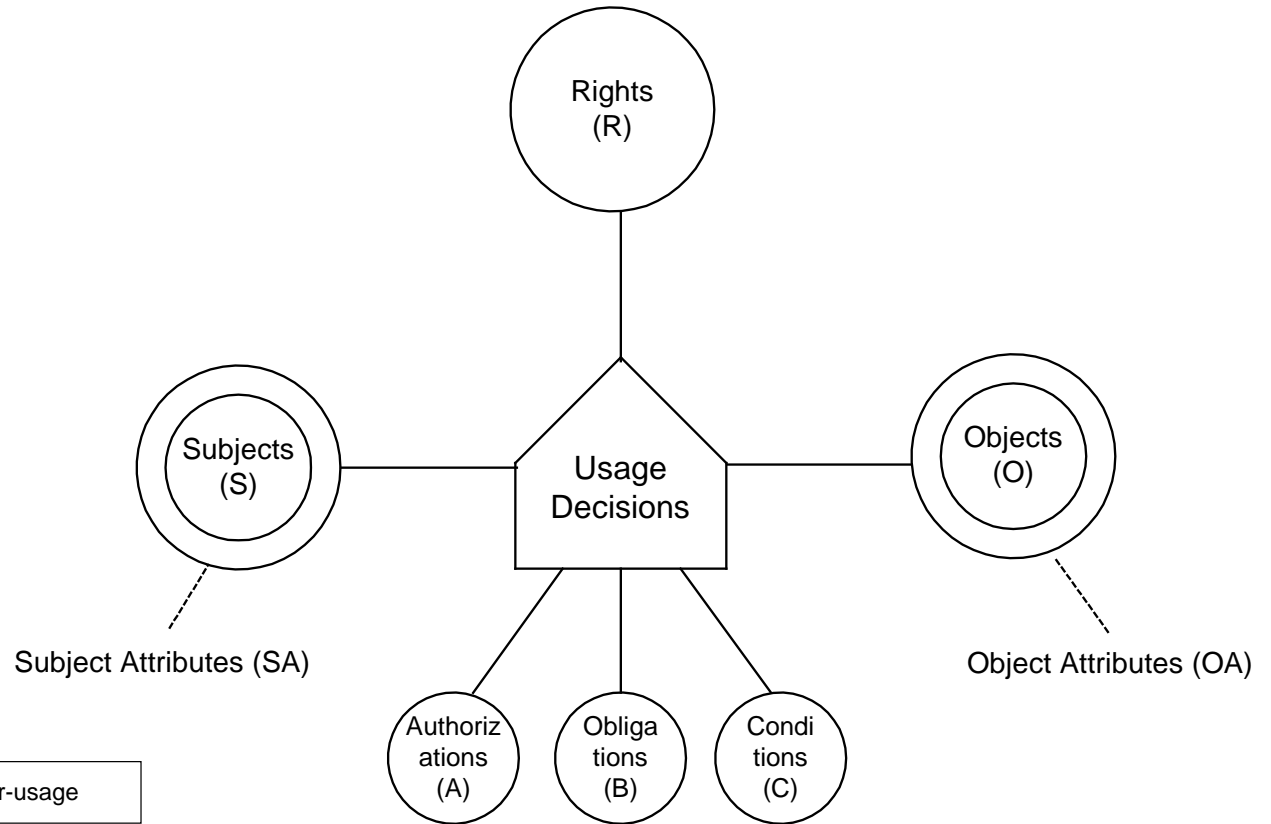
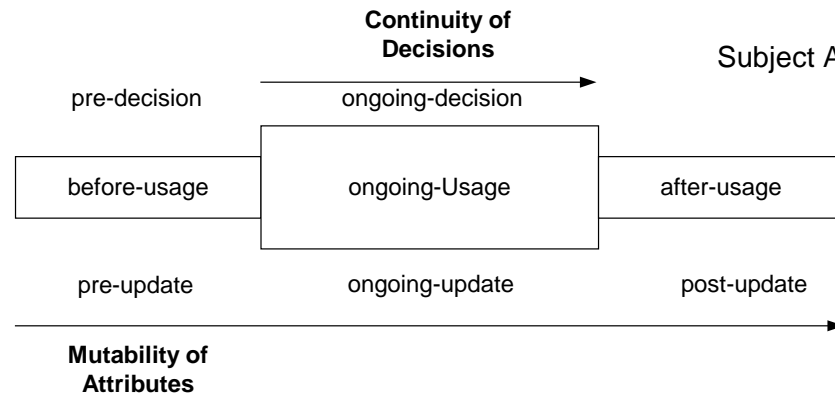
Mature Internet, 2000s

Attributes

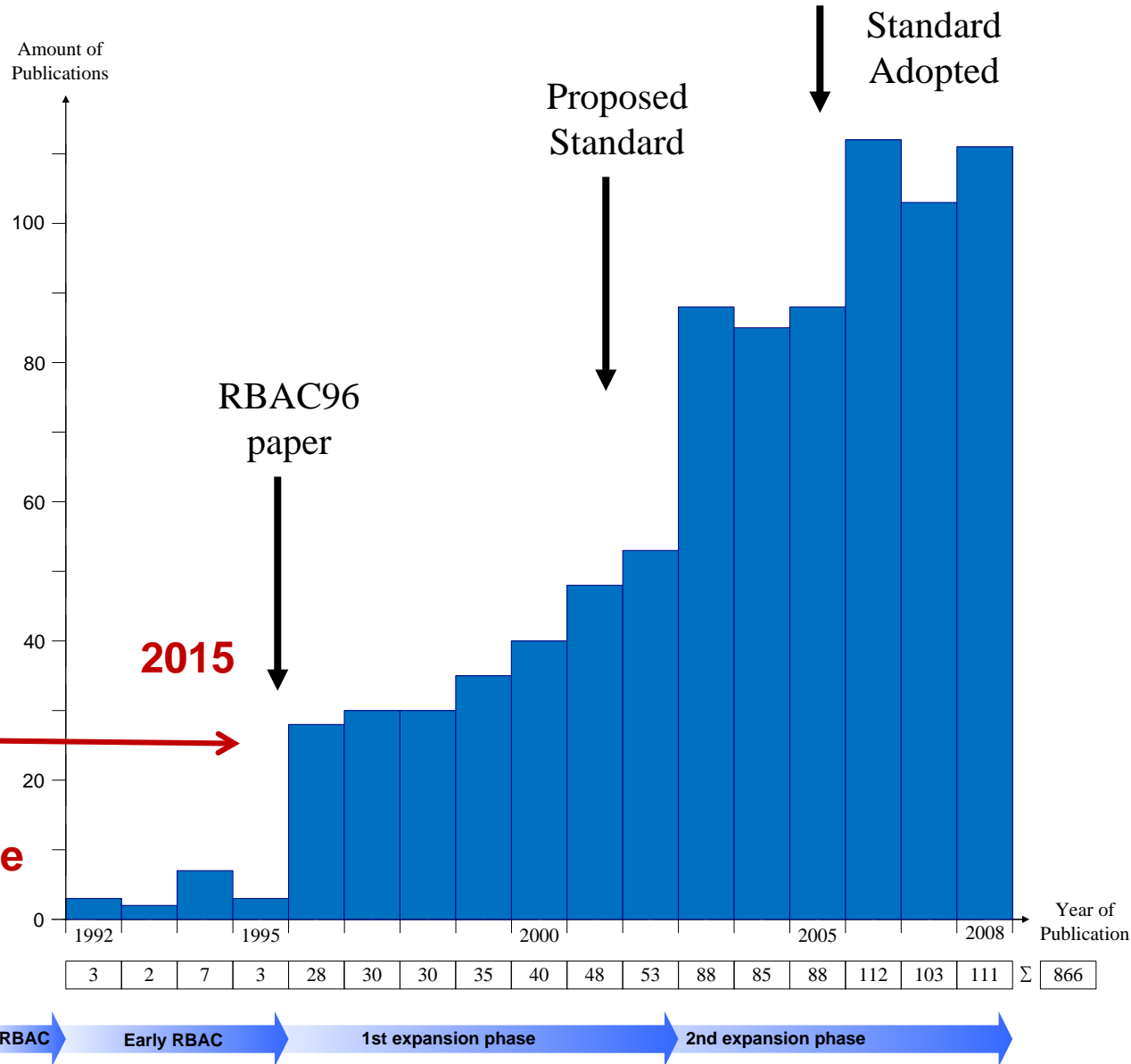


Mature Internet, 2000s

- unified model integrating
 - authorization
 - obligation
 - conditions
- and incorporating
 - continuity of decisions
 - mutability of attributes

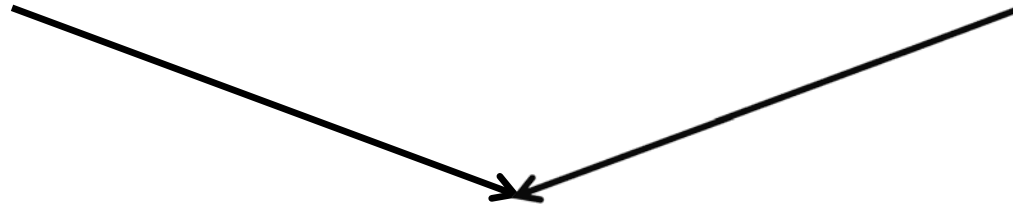


Usage Control Models, early 2000s



**Discretionary Access Control
(DAC), 1970**

**Mandatory Access Control
(MAC), 1970**

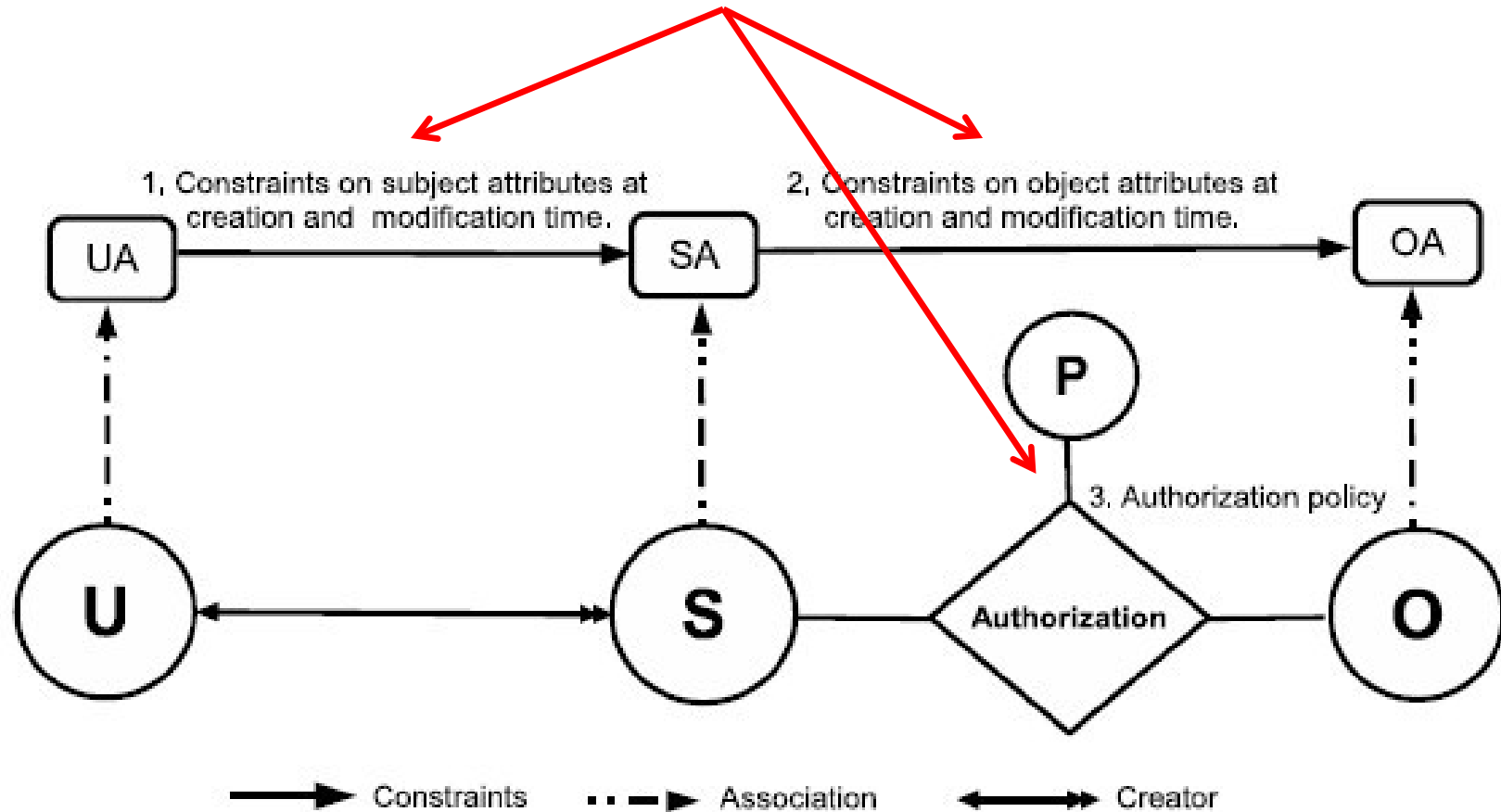


**Role Based Access Control
(RBAC), 1995**



**Attribute Based Access Control
(ABAC), ????**

Policy Configuration Points



**Can be configured to do simple forms of
DAC, MAC, RBAC**

1, 2, 4, 5

Extended Constraints on Role Activation:

Attribute-Based User-Role Assignment- 2002 [6], OASIS-RBAC-2002 [9], SRBAC-2003 [46], Rule-RBAC-2004 [5], GEO-RBAC-2005 [16]

1,4

Extended Concept of Role:

Role Template-1997 [45], Parameterized RBAC-2004 [2], Parameterized RBAC-2003 [34], Parameterized Role-2004 [43], Attributed Role-2006 [99]

1, 4, 5

Changes in Role-Permission Relationship:

Task-RBAC-2000 [77], Task-RBAC-2003 [78]

4, 5

Organization and Team:

Relationship-RBAC -1997 [12], TeamMAC-1997 [87], TeamMAC-2004 [7], ROBAC-2006 [103], Group-RBAC-2009 [66], RABAC-2013 [51], Domain-RBAC -2013 [98]

4

1, 4, 5

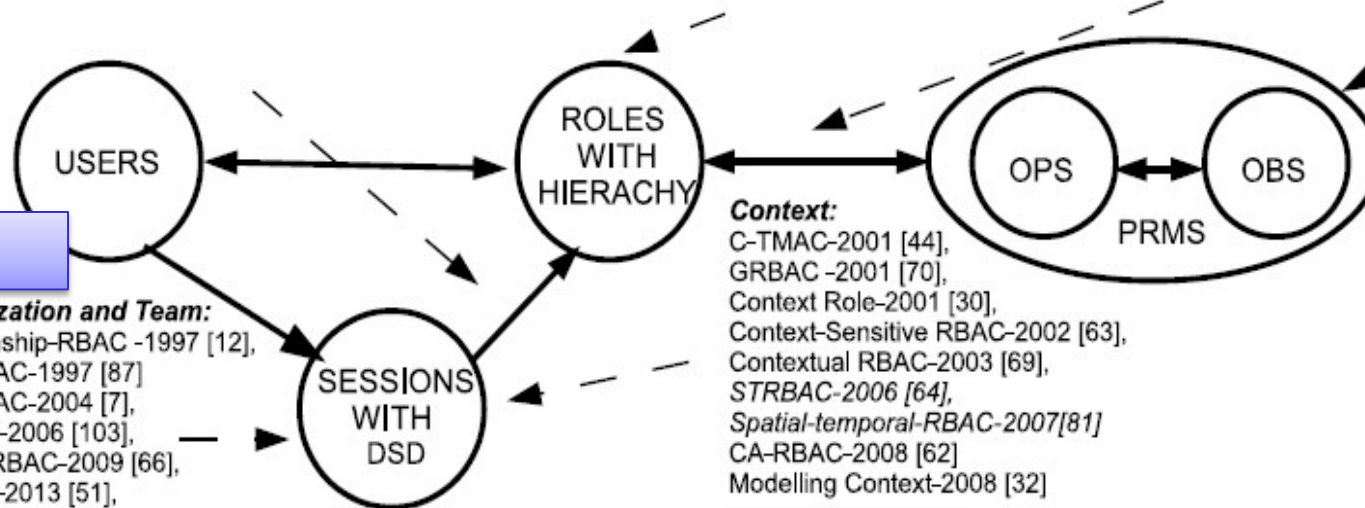
Context:

C-TMAC-2001 [44], GRBAC -2001 [70], Context Role-2001 [30], Context-Sensitive RBAC-2002 [63], Contextual RBAC-2003 [69], STRBAC-2006 [64], Spatial-temporal-RBAC-2007[81], CA-RBAC-2008 [62], Modelling Context-2008 [32]

Extended Permission Structure:

RBAC with Object class- 2007 [24], Conditional PRBAC 07 [74], PRBAC 07 [75], Purpose-aware RBAC- 2008 [67], Ubi-RBAC-2010 [76], RCPBAC-2011 [55]

1, 2, 3, 4, 5



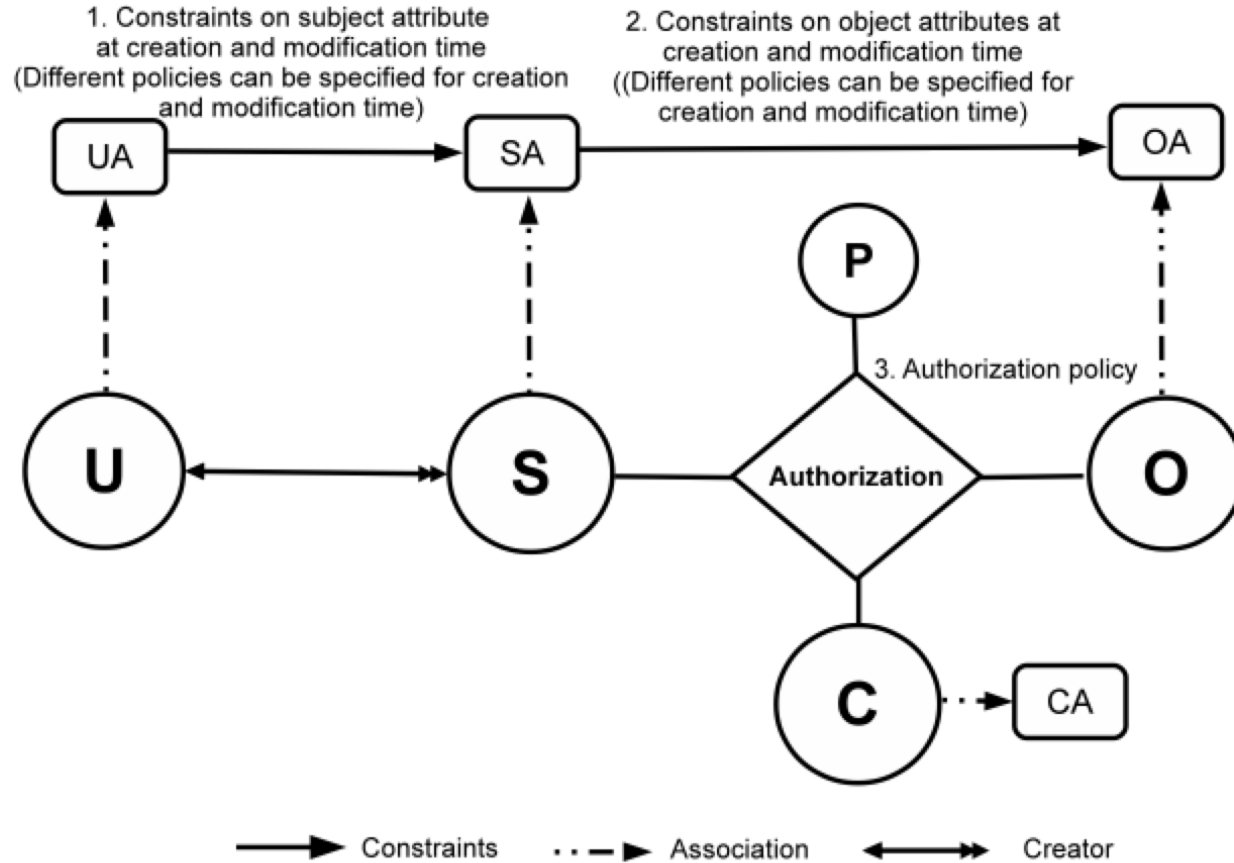
1. Context Attributes

2. Subject attribute constraints policy are different at creation and modification time.

3. Subject attributes constrained by attributes of subjects created by the same user.

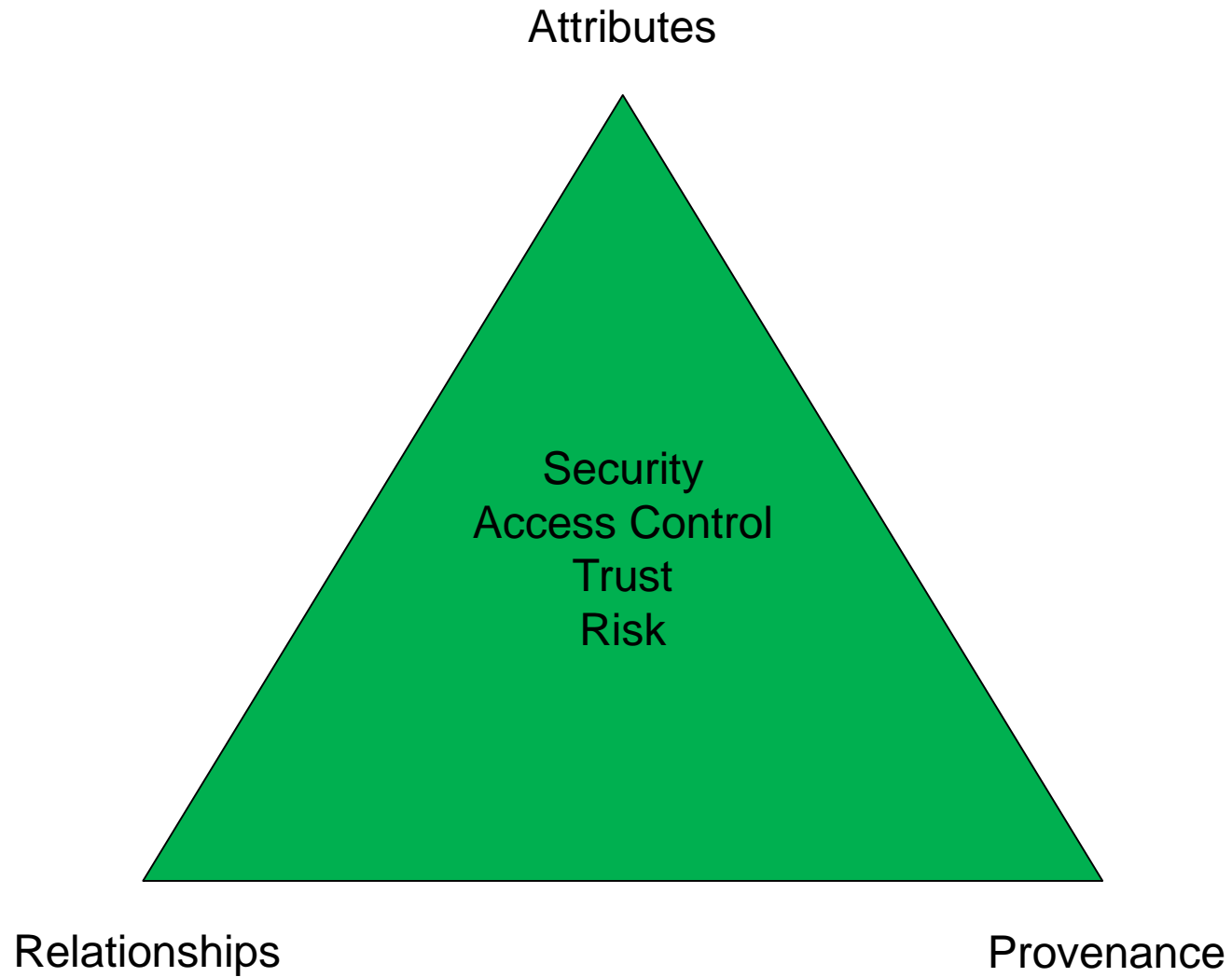
4. Policy Language

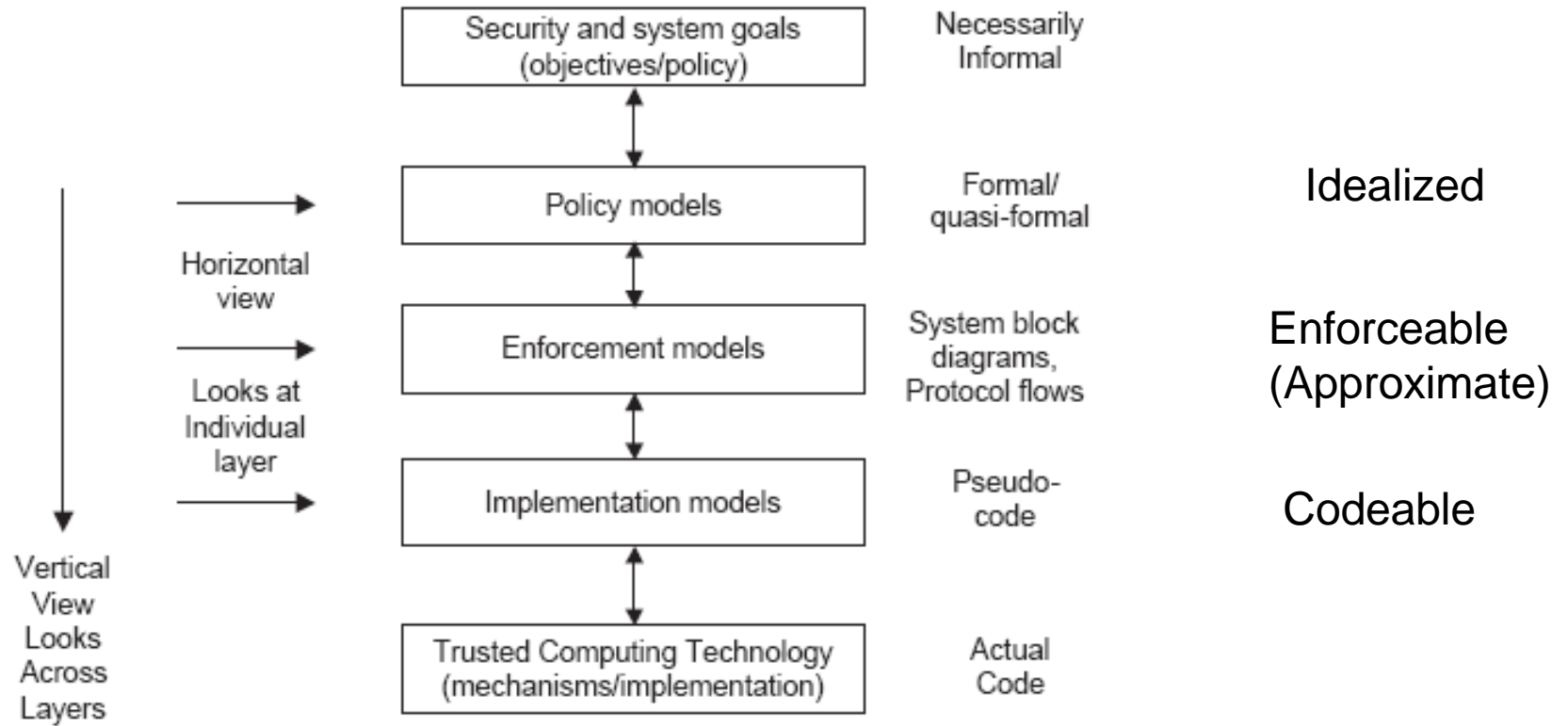
5. Meta-Attributes

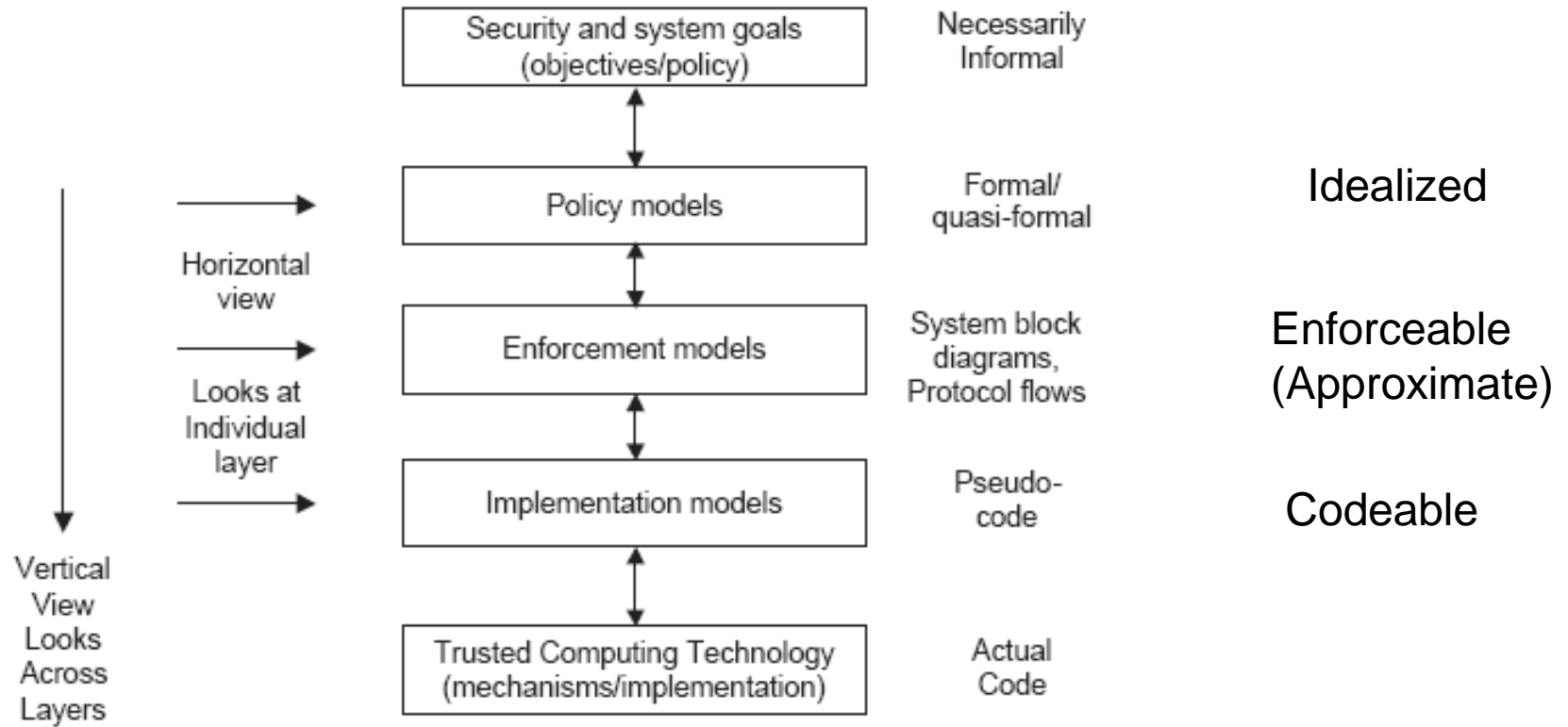


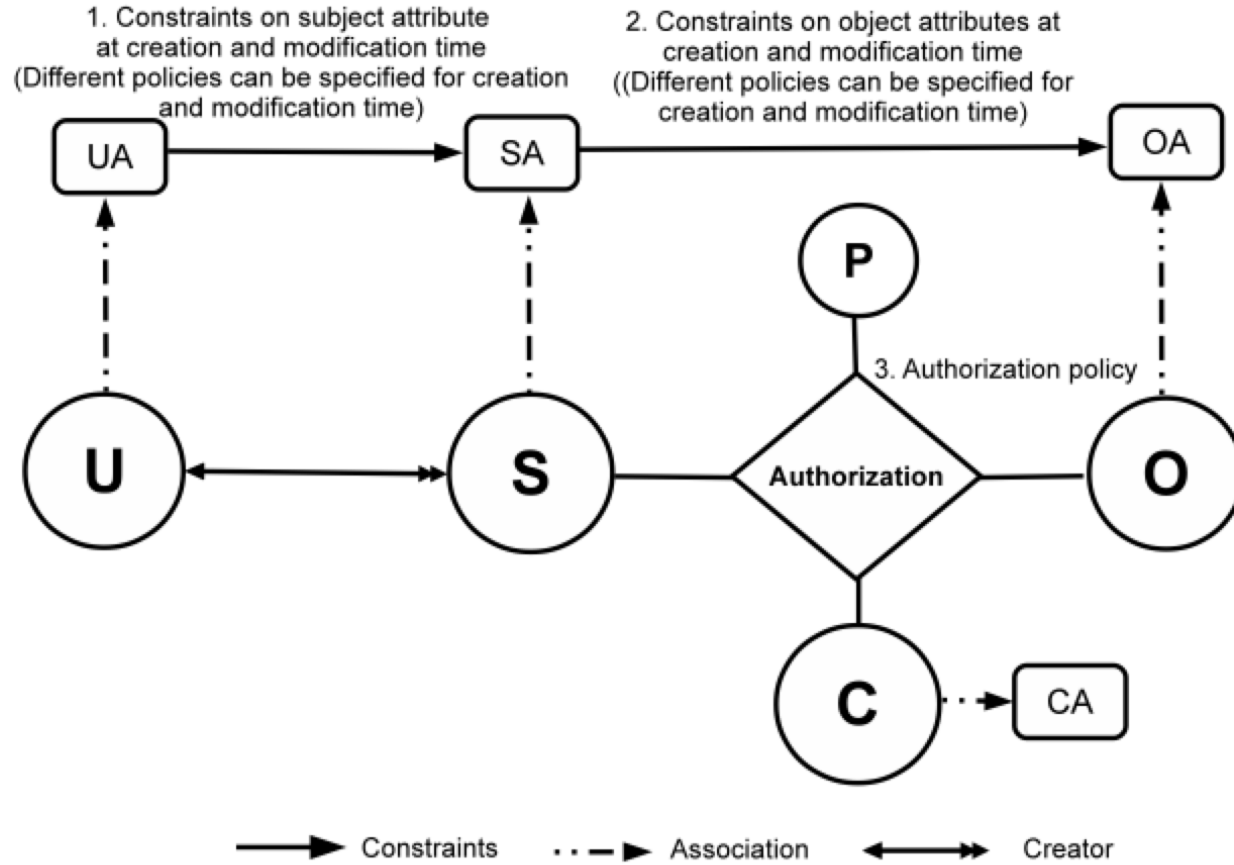
Can be configured to do many RBAC extensions

SOME RESEARCH CHALLENGES





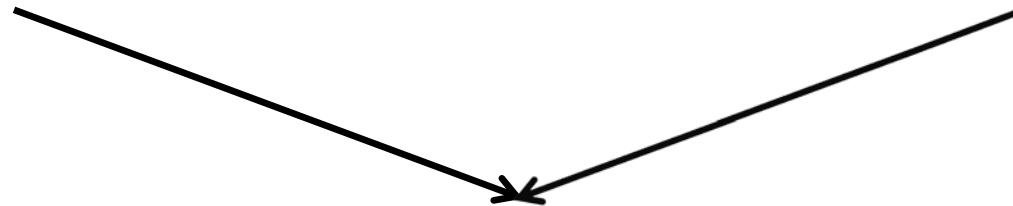




- Cloud computing
- Internet of Things
-

**Discretionary Access Control
(DAC), 1970**

**Mandatory Access Control
(MAC), 1970**



**Role Based Access Control
(RBAC), 1995**



**Attribute Based Access Control
(ABAC), ????**