# Attribute-Based Access Control Models and Beyond

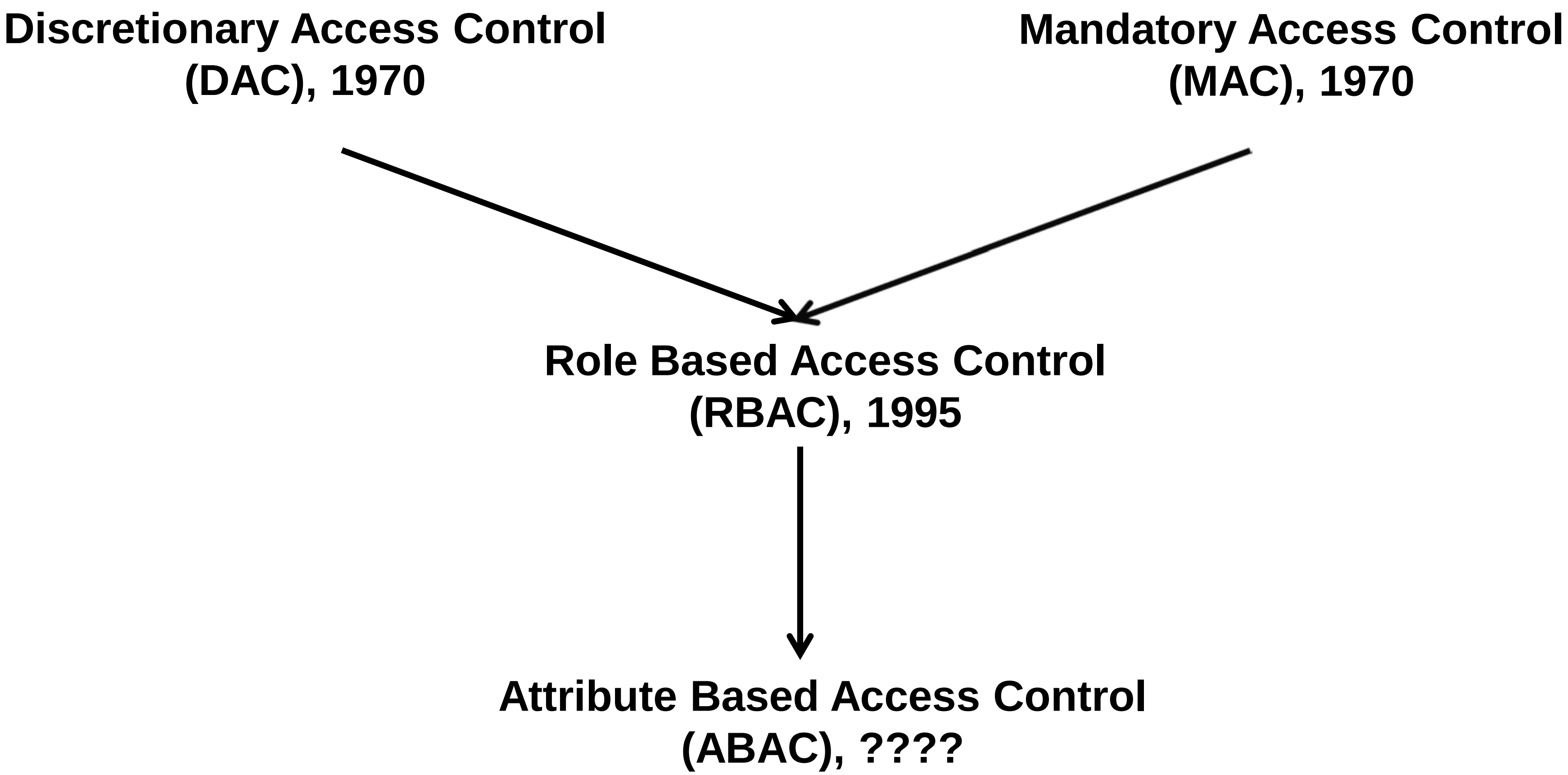
Prof. Ravi Sandhu

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

Indraprastha Institute of Information Technology (IIIT), Delhi
February 14, 2015

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

# Access Control



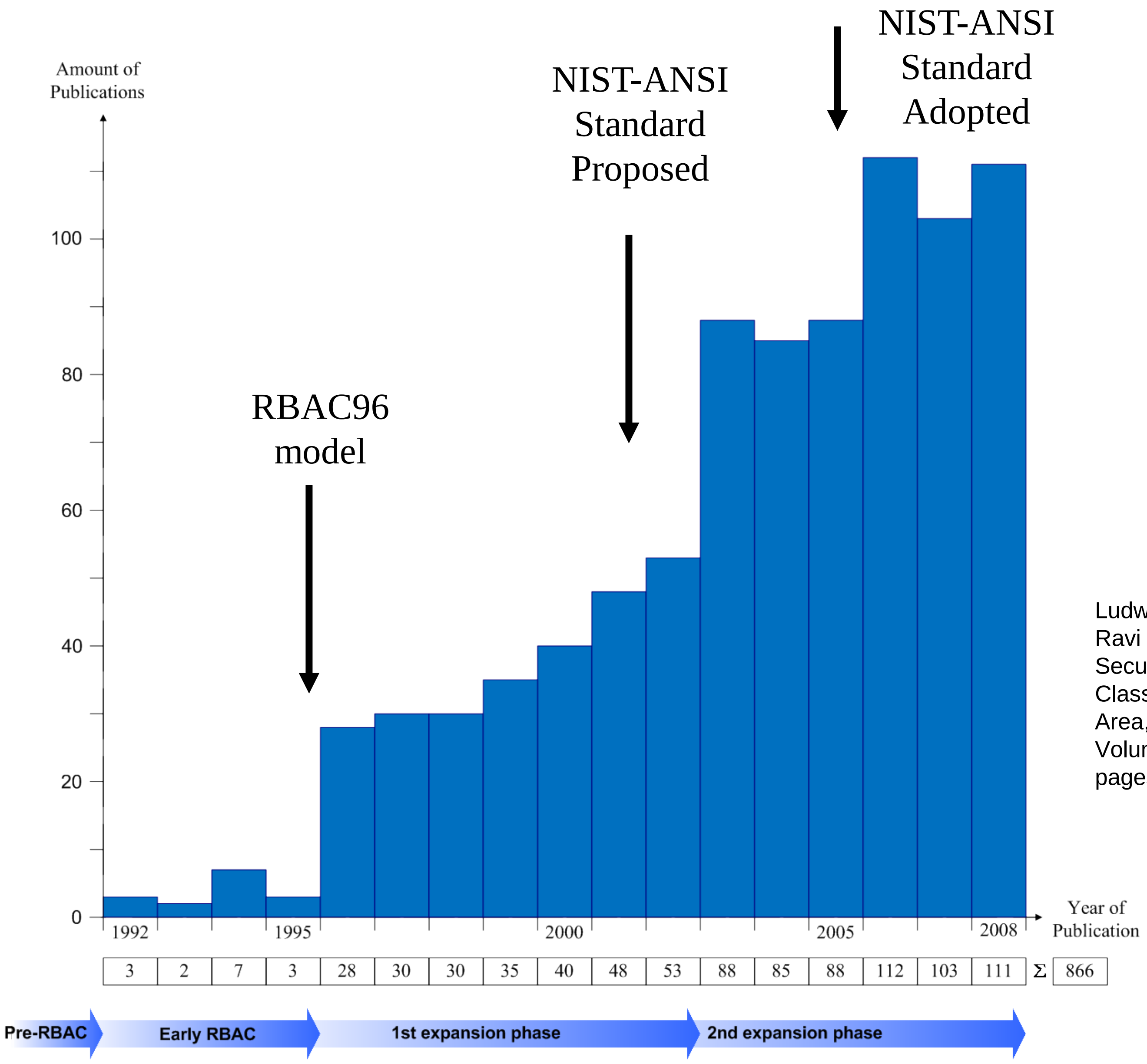
Discretionary Access Control (DAC), 1970

Mandatory Access Control (MAC), 1970

Role Based Access Control (RBAC), 1995

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

# The RBAC Story



RBAC96 model

NIST-ANSI Standard Proposed

NIST-ANSI Standard Adopted

Pre-RBAC

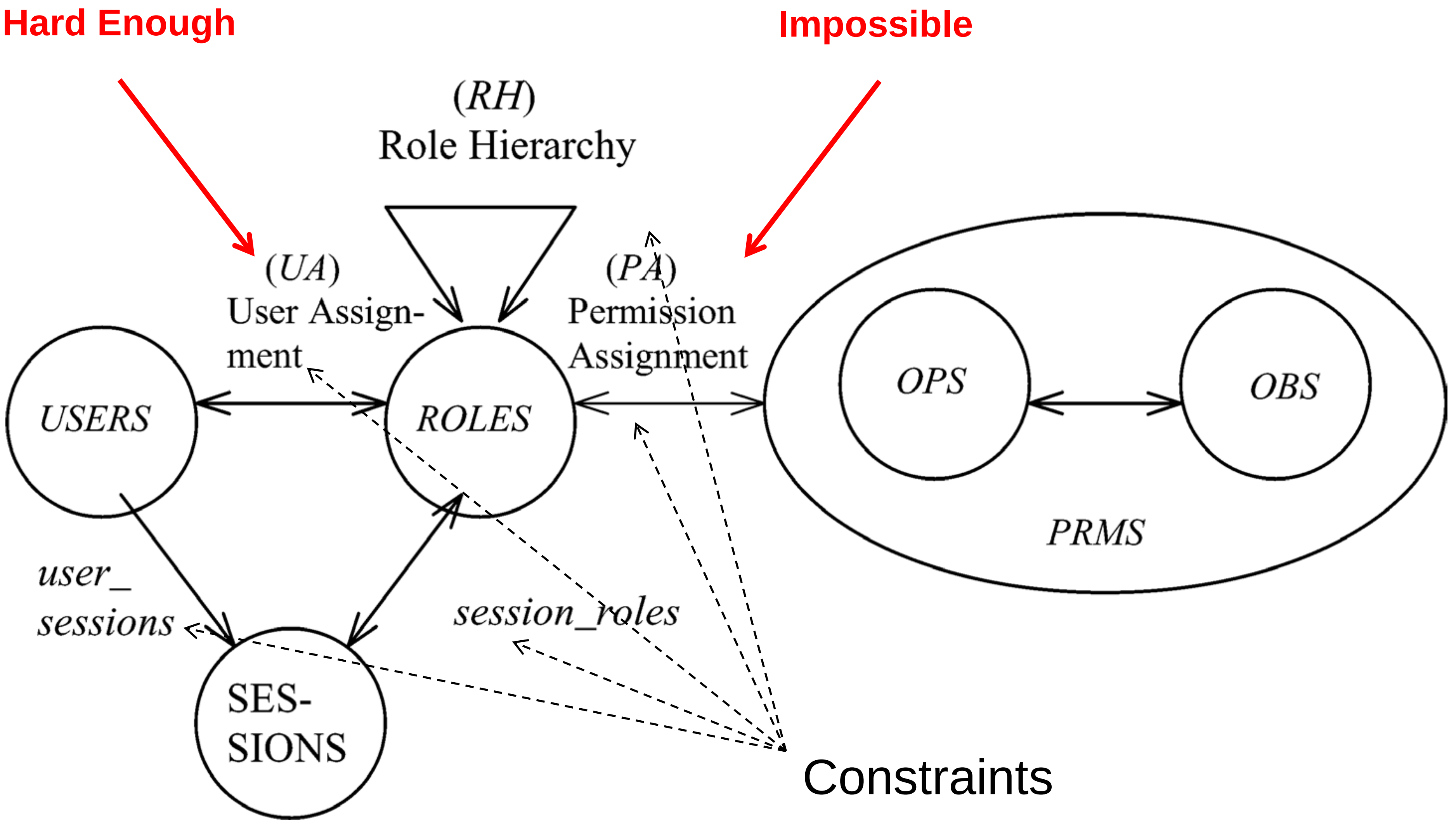
Early RBAC

1st expansion phase

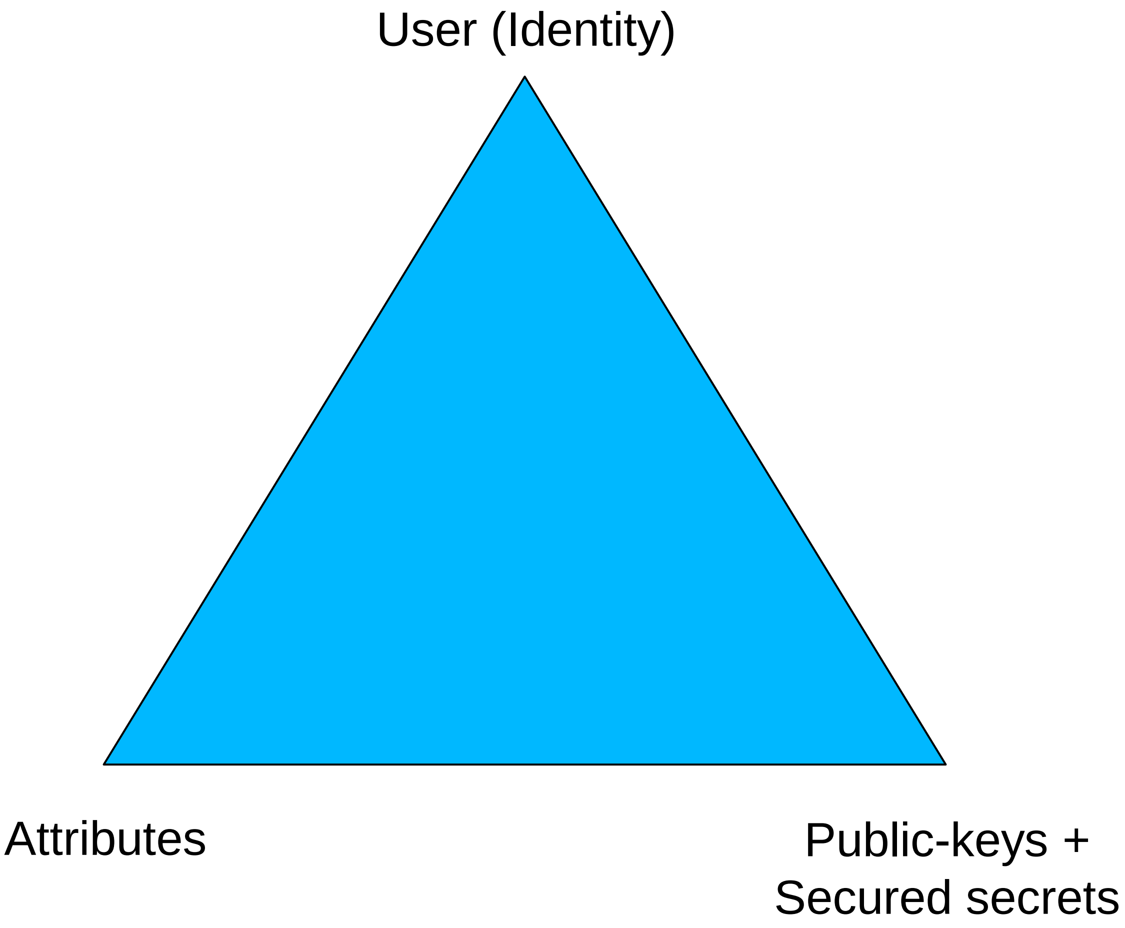
2nd expansion phase

Ludwig Fuchs, Gunther Pernul and Ravi Sandhu, Roles in Information Security-A Survey and Classification of the Research Area, Computers & Security, Volume 30, Number 8, Nov. 2011, pages 748-76

# RBAC Shortcomings



# ABAC is not New

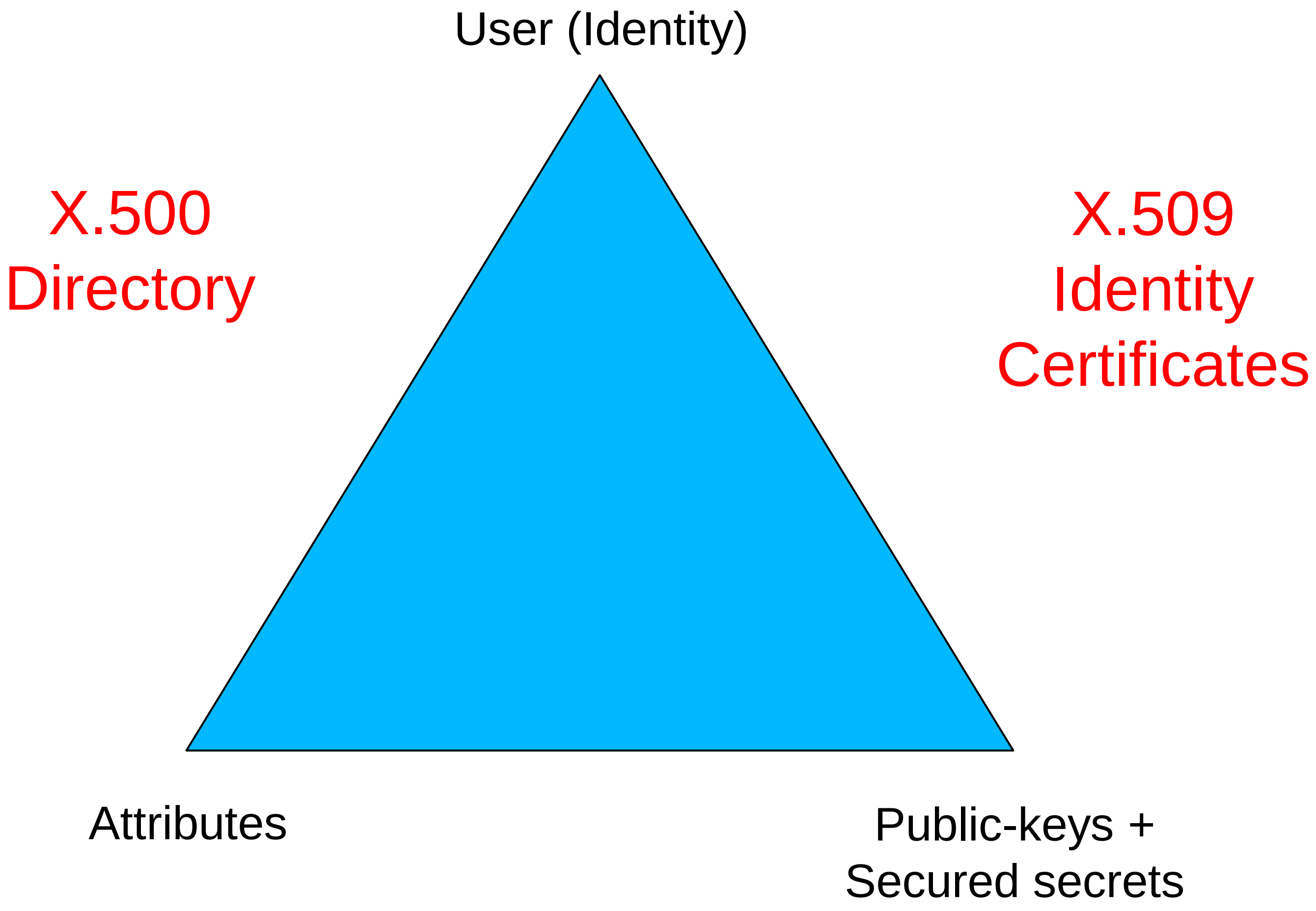


User (Identity)

Attributes

Public-keys +
Secured secrets

# ABAC is not New


User (Identity)

X.500 Directory

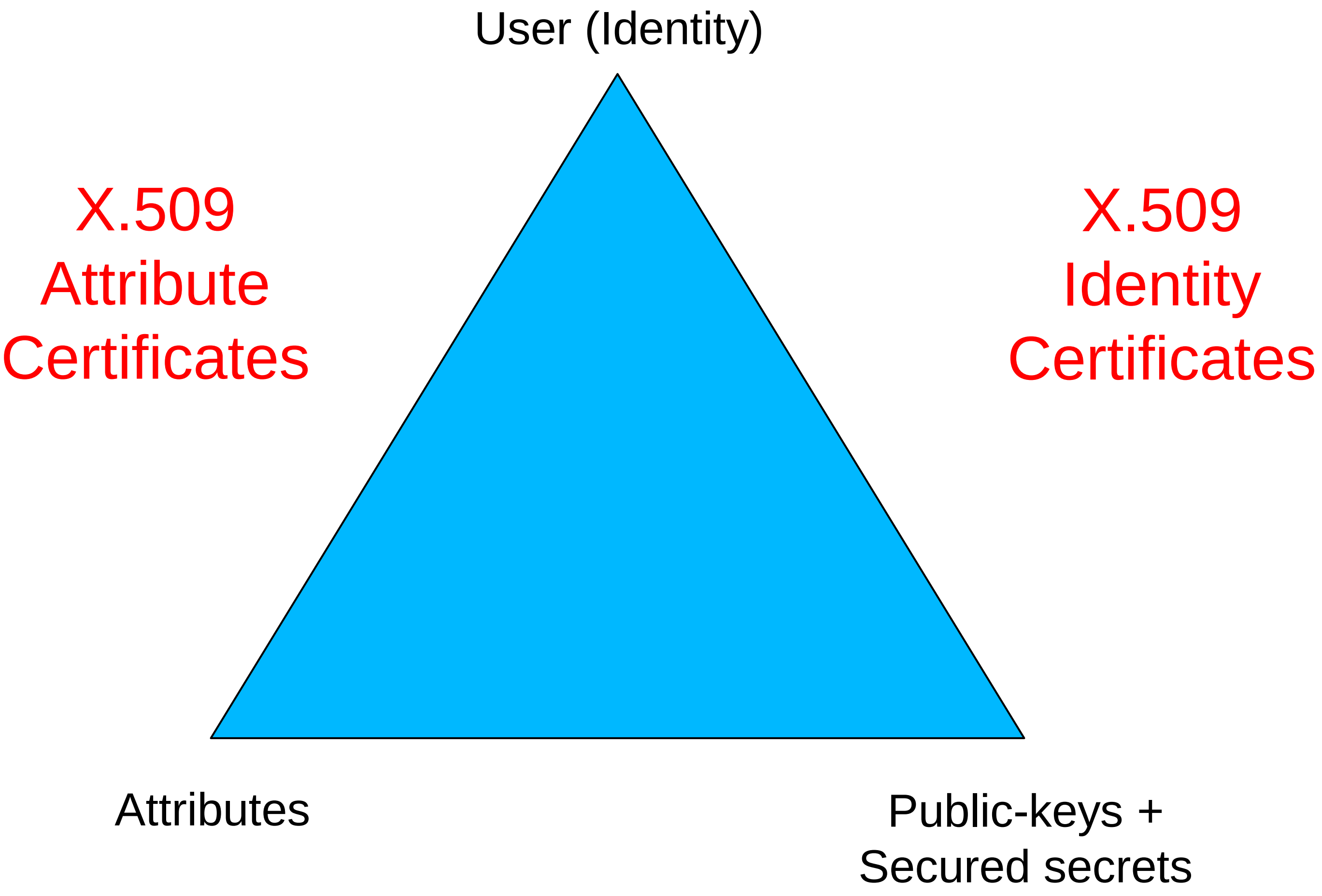
X.509 Identity Certificates

Attributes

Public-keys + Secured secrets

Pre Internet, early 1990s

# ABAC is not New



User (Identity)

X.509 Attribute Certificates

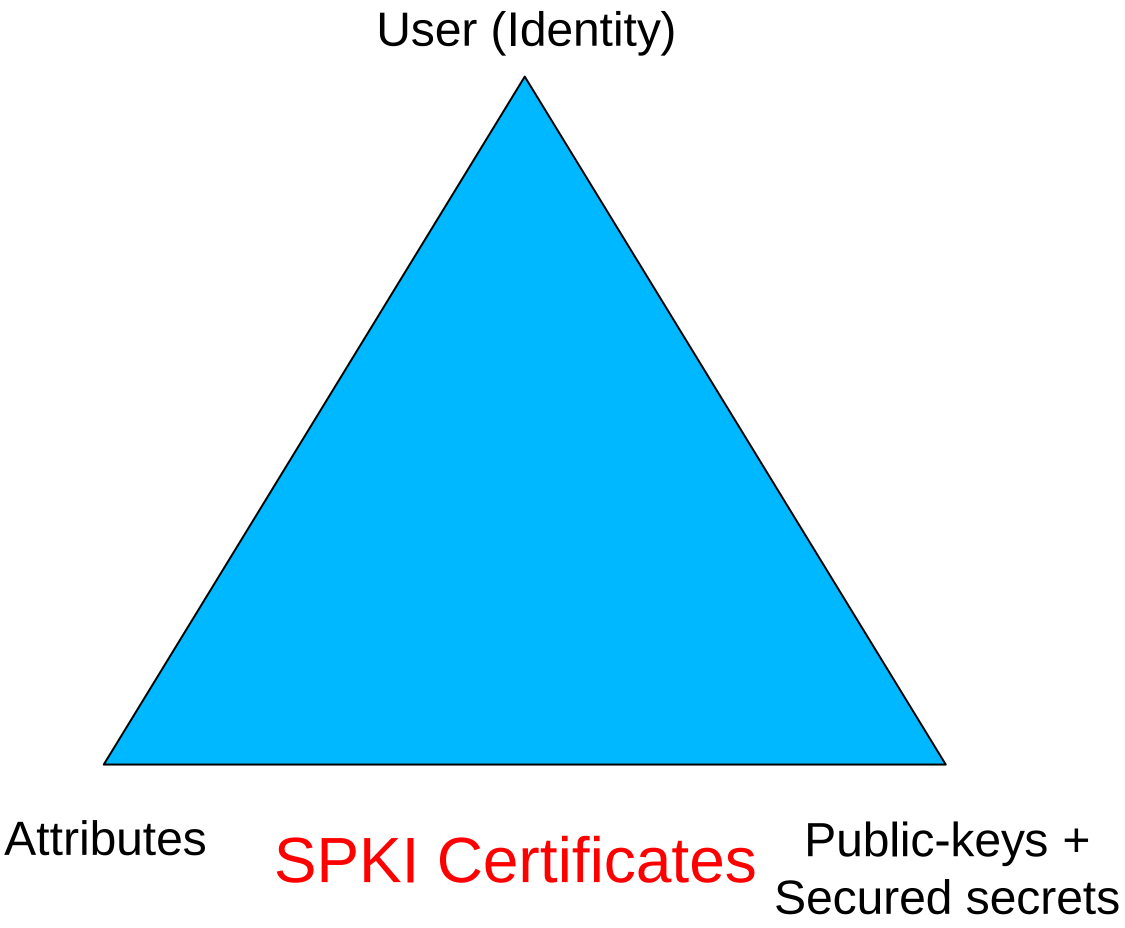
X.509 Identity Certificates

Attributes

Public-keys + Secured secrets

Post Internet, late 1990s

# ABAC is not New



User (Identity)

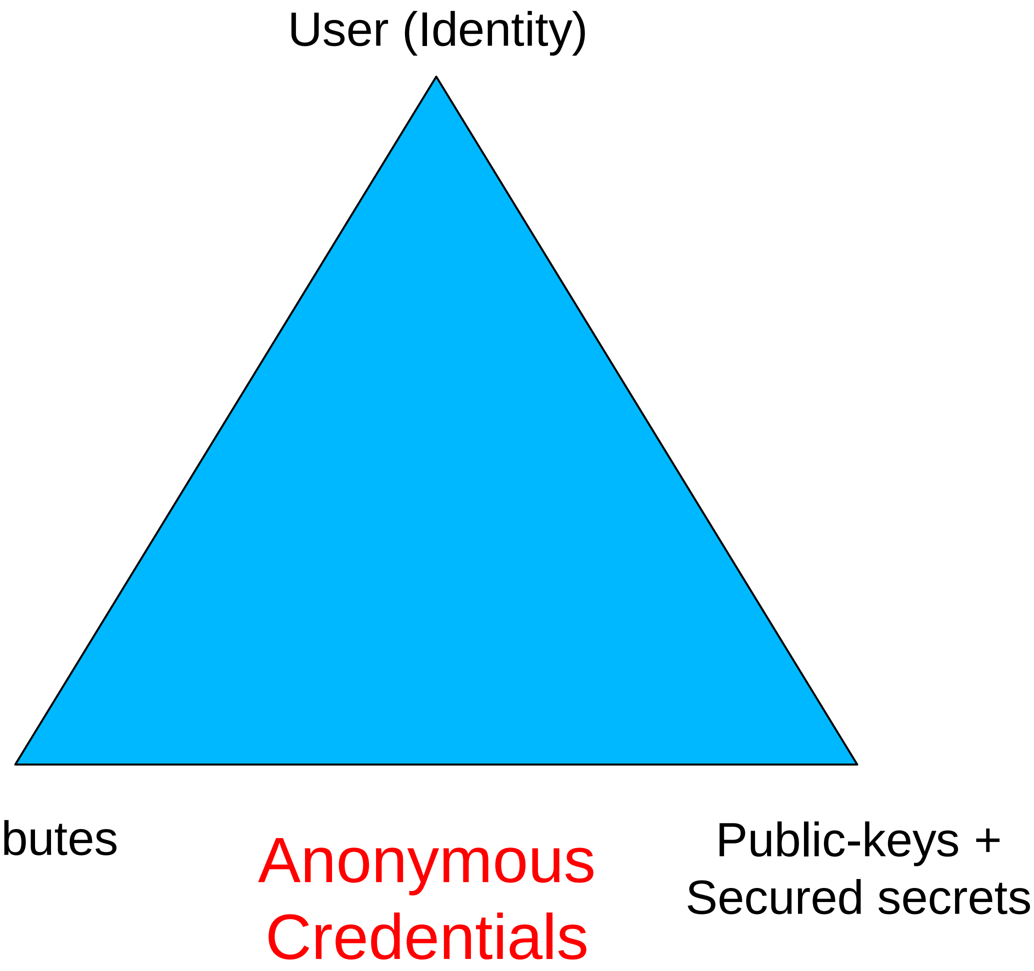
Attributes

SPKI Certificates

Public-keys +
Secured secrets

Post Internet, late 1990s

# ABAC is not New


User (Identity)

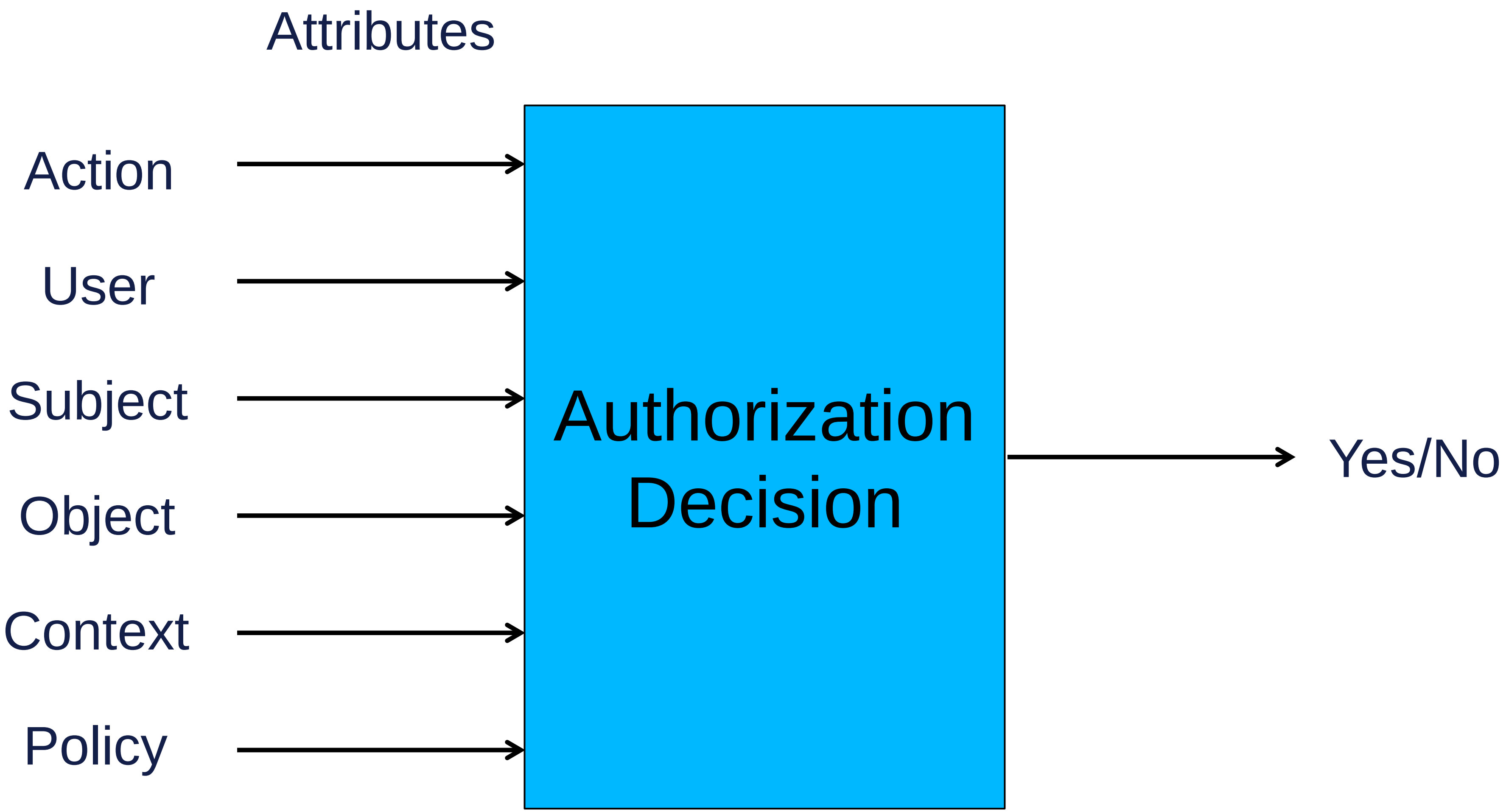
Attributes

Anonymous Credentials

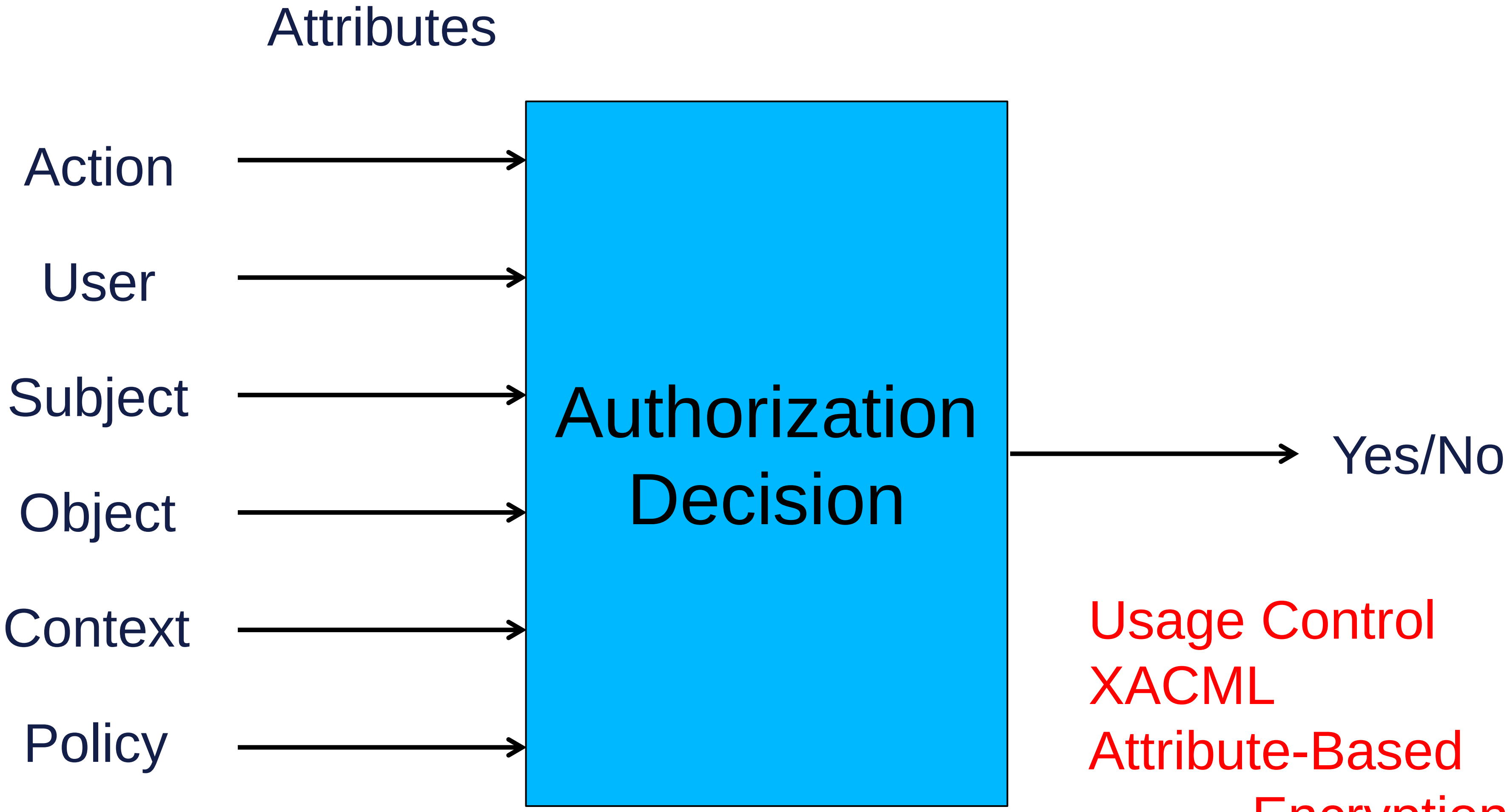
Public-keys + Secured secrets

Mature Internet, 2000s

# ABAC is not New



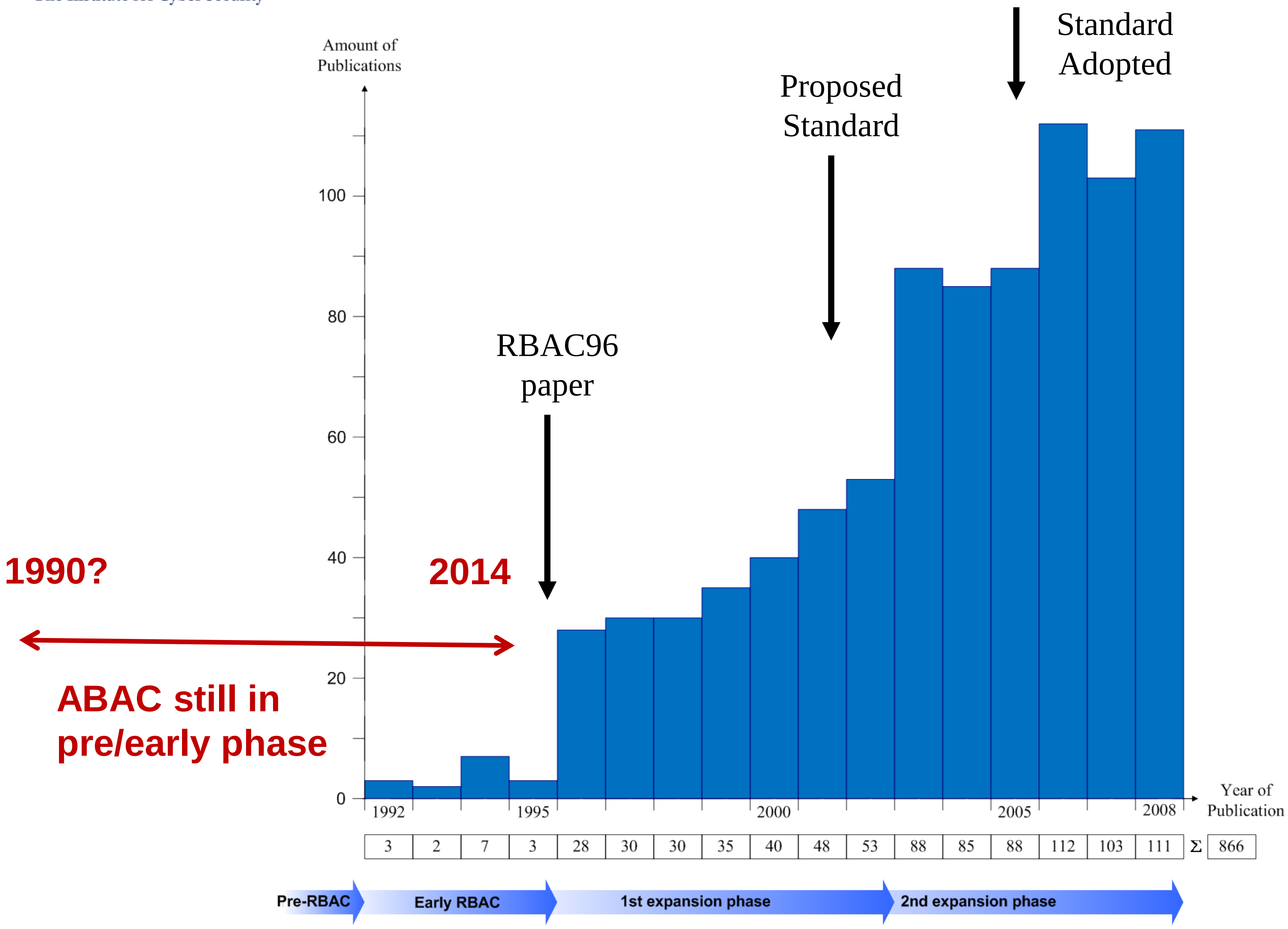
# ABAC is not New



Usage Control
XACML
Attribute-Based Encryption

Mature Internet, 2000s

# ABAC Status



**1990?**

**2014**

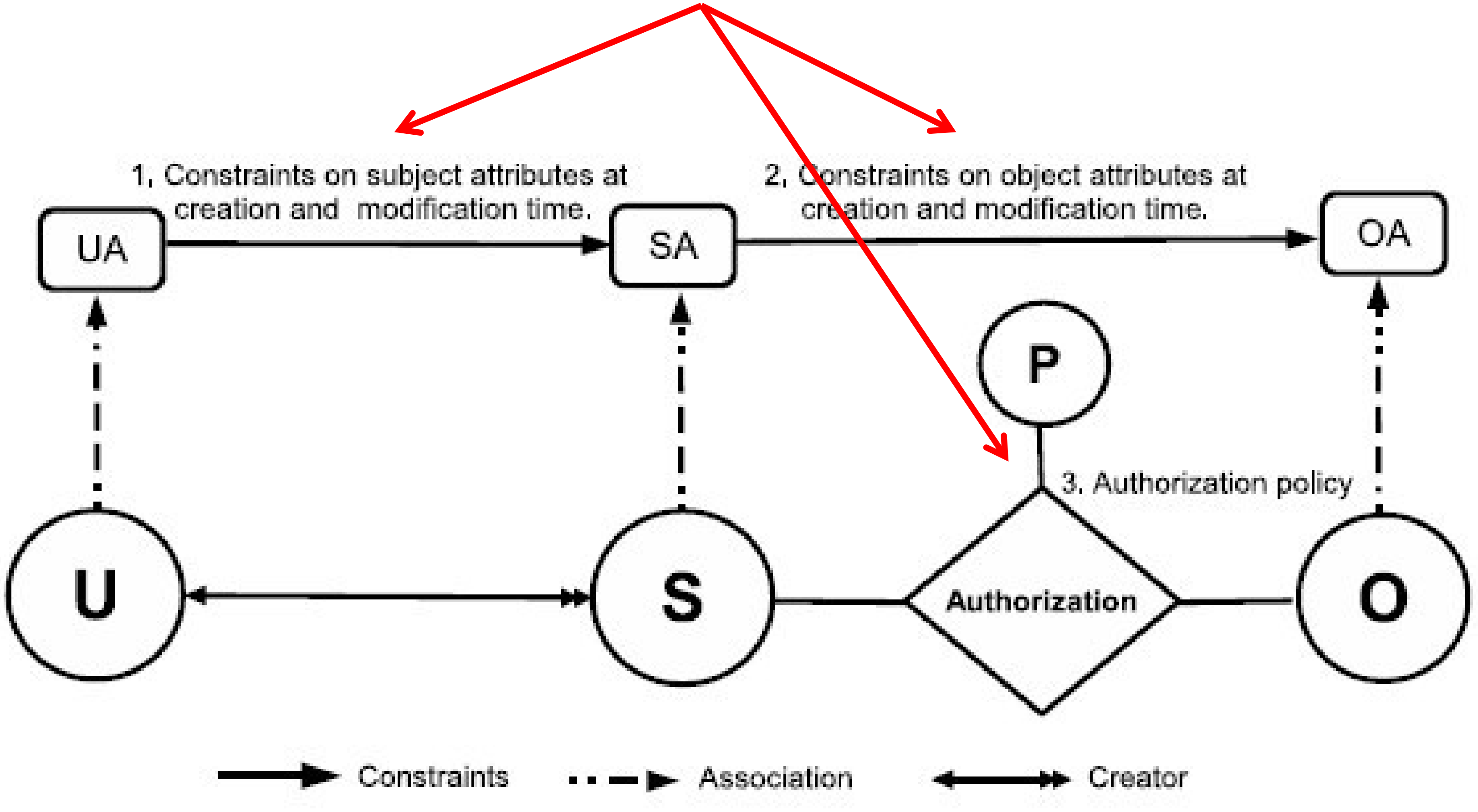
**ABAC still in pre/early phase**

# Attribute-Based Access Control (ABAC)

- Attributes are name:value pairs
  - possibly chained
  - values can be complex data structures
- Associated with
  - actions
  - users
  - subjects
  - objects
  - contexts
  - policies
- Converted by policies into rights just in time
  - policies specified by security architects
  - attributes maintained by security administrators
  - but also possibly by users OR reputation and trust mechanisms
- Inherently extensible

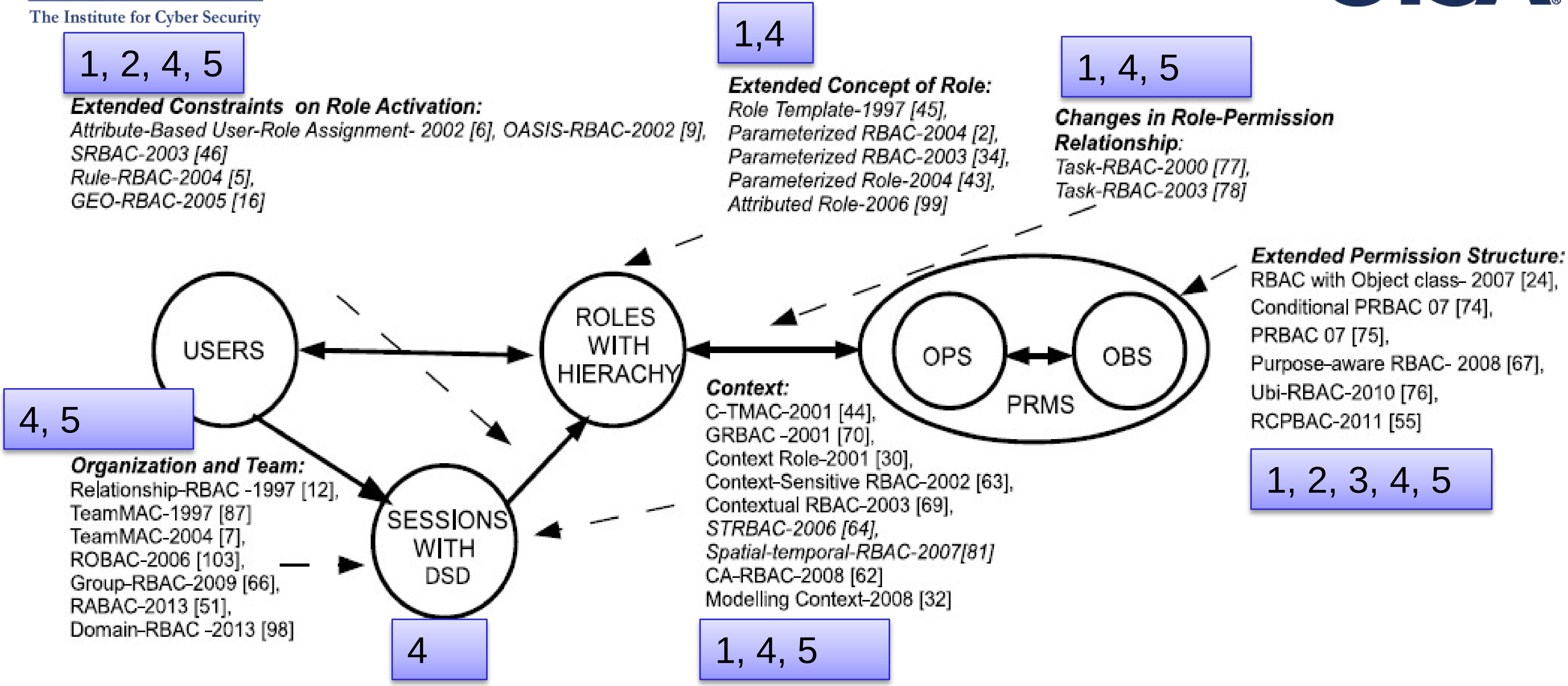
# ABACα Model Structure

Policy Configuration Points


1, Constraints on subject attributes at creation and modification time.
2, Constraints on object attributes at creation and modification time.
UA
SA
OA
P
3. Authorization policy
U
S
Authorization
O
Constraints
Association
Creator

Can be configured to do DAC, MAC, RBAC

# ABAC$_\beta$ Scope



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]*

***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

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

***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]

1, 4, 5

1. Context Attributes

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

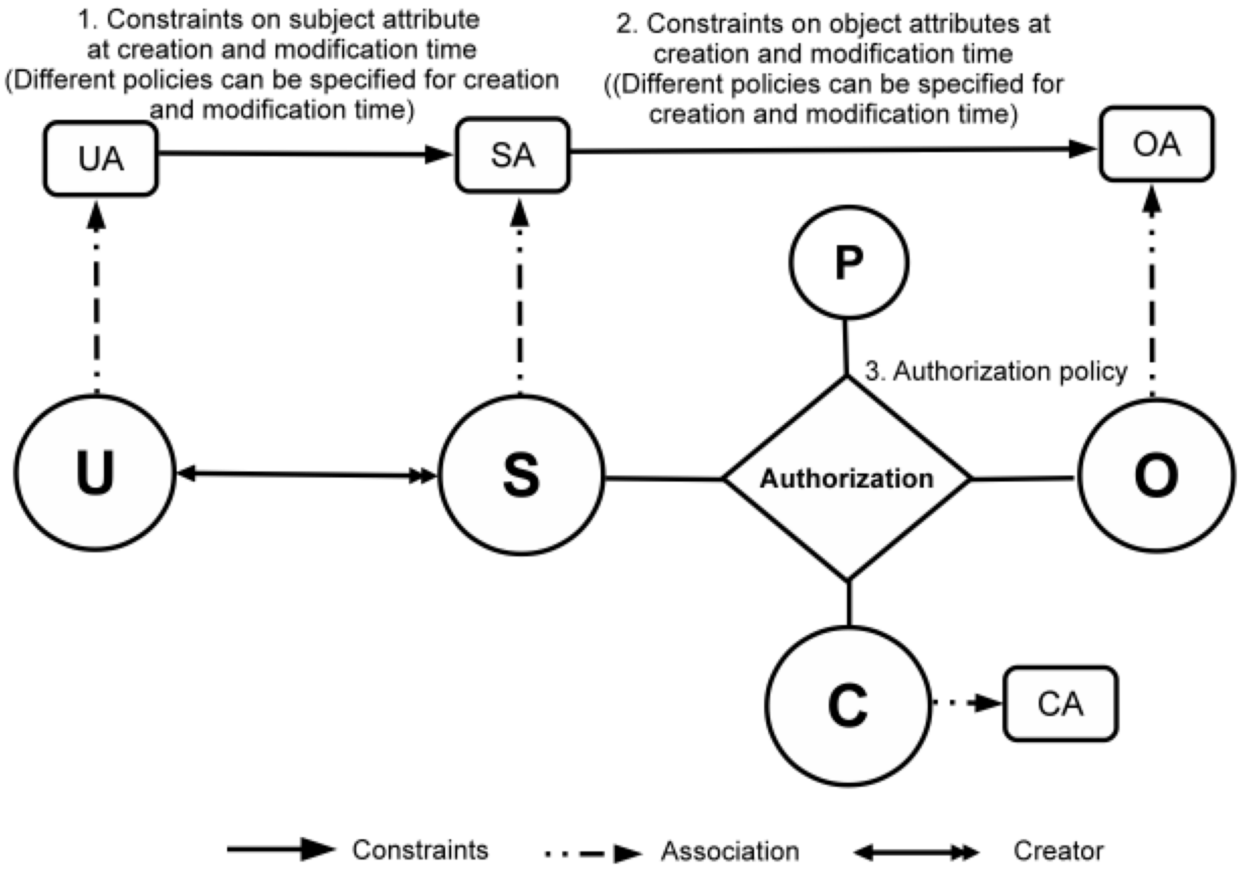
3. Subject attributes constrained by attributes of subjects created by the same user.

4. Policy Language

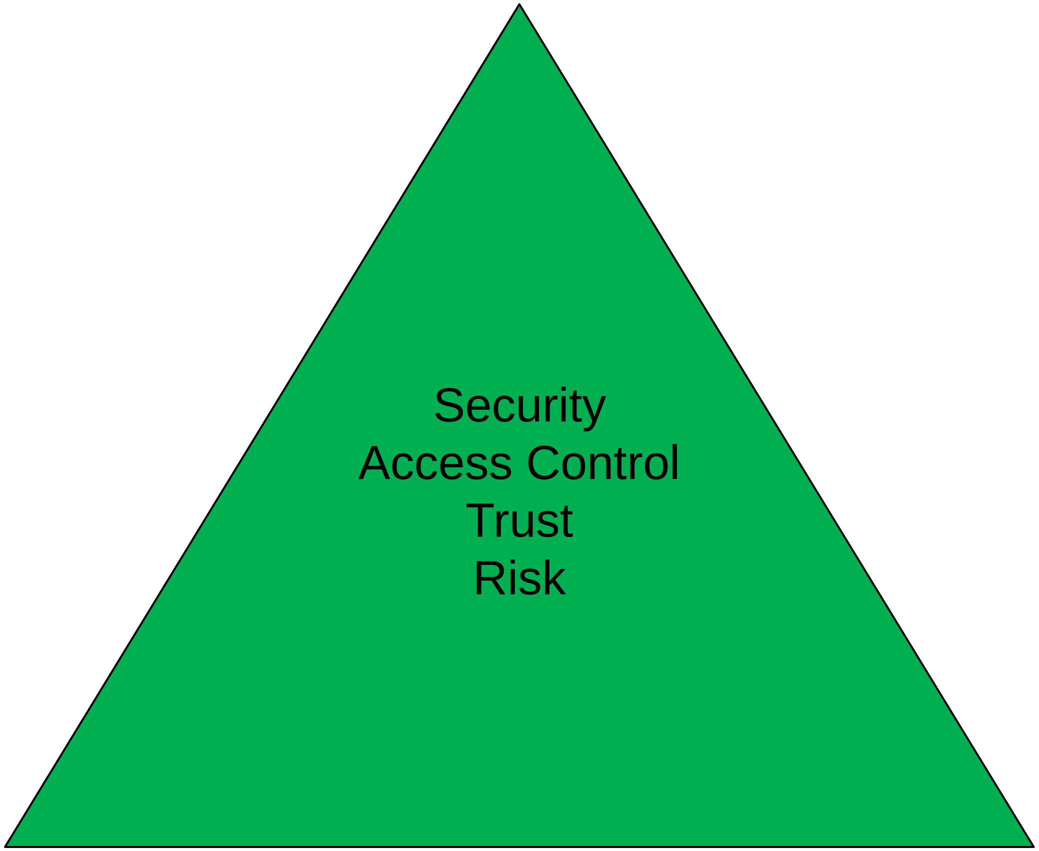
5. Meta-Attributes

*World-Leading Research with Real-World Impact!*

# ABAC$_{\beta}$ Model


1. Constraints on subject attribute at creation and modification time (Different policies can be specified for creation and modification time)
2. Constraints on object attributes at creation and modification time ((Different policies can be specified for creation and modification time)
UA
SA
OA
P
3. Authorization policy
U
S
Authorization
O
C
CA
Constraints
Association
Creator

# Beyond ABAC



Attributes

Security
Access Control
Trust
Risk

Relationships

Provenance

# ABAC Research at ICS

- GURA model for user-attribute assignment
- Safety analysis of $ABAC_\alpha$ and $ABAC_\beta$
- Undecidable safety for ABAC models
- Decidable safety for ABAC with finite fixed attributes
- Constraints in ABAC
- ABAC Cloud IaaS implementations (OpenStack)
- Attribute Engineering
- Attribute Mining
- Unification of Attributes, Relationships and Provenance