



idm IDENTITY
MANAGEMENT
TESTBED

Attribute based access control data models for ICAM



**Homeland
Security**

Science and Technology

Thomas.Smith@jhuapl.edu
Maria.Vachino@jhuapl.edu

Outline

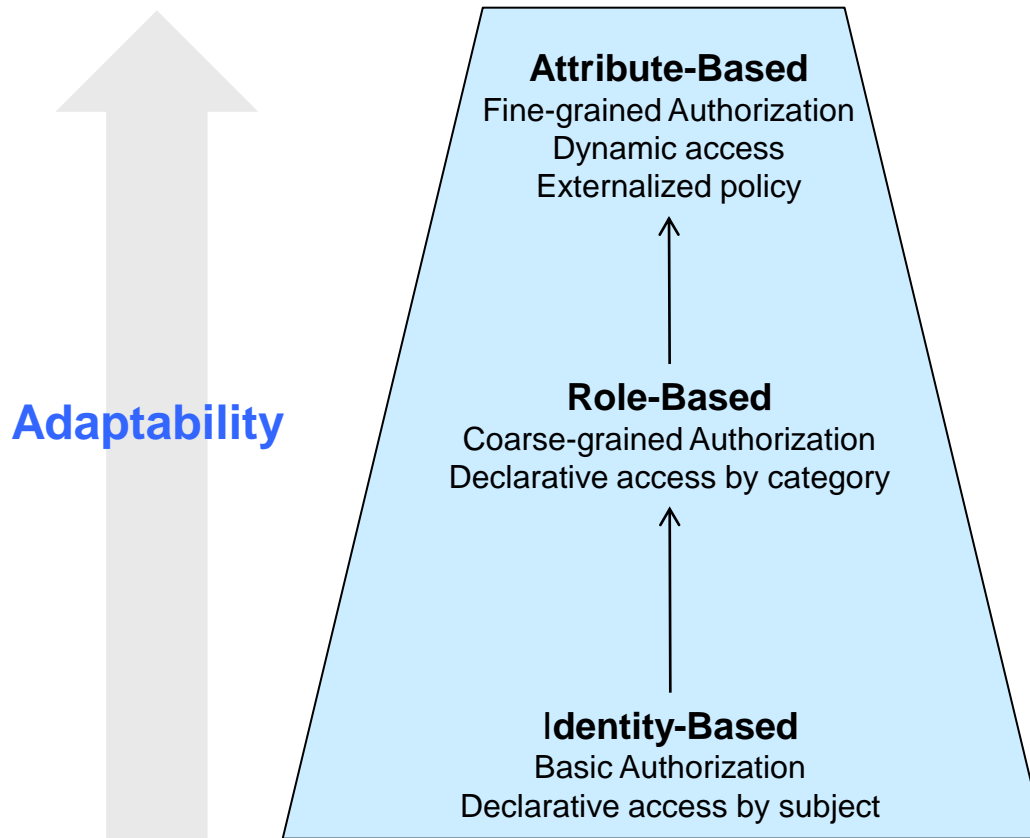
- Problem Domain
- Concept Modeling
 - Semantic Consensus
 - Attribute & policy alignment
 - Focus
- ICAM Concept Model
- Existing Effort Mappings
- Logical Model
- Physical Model

Access Control Essentials

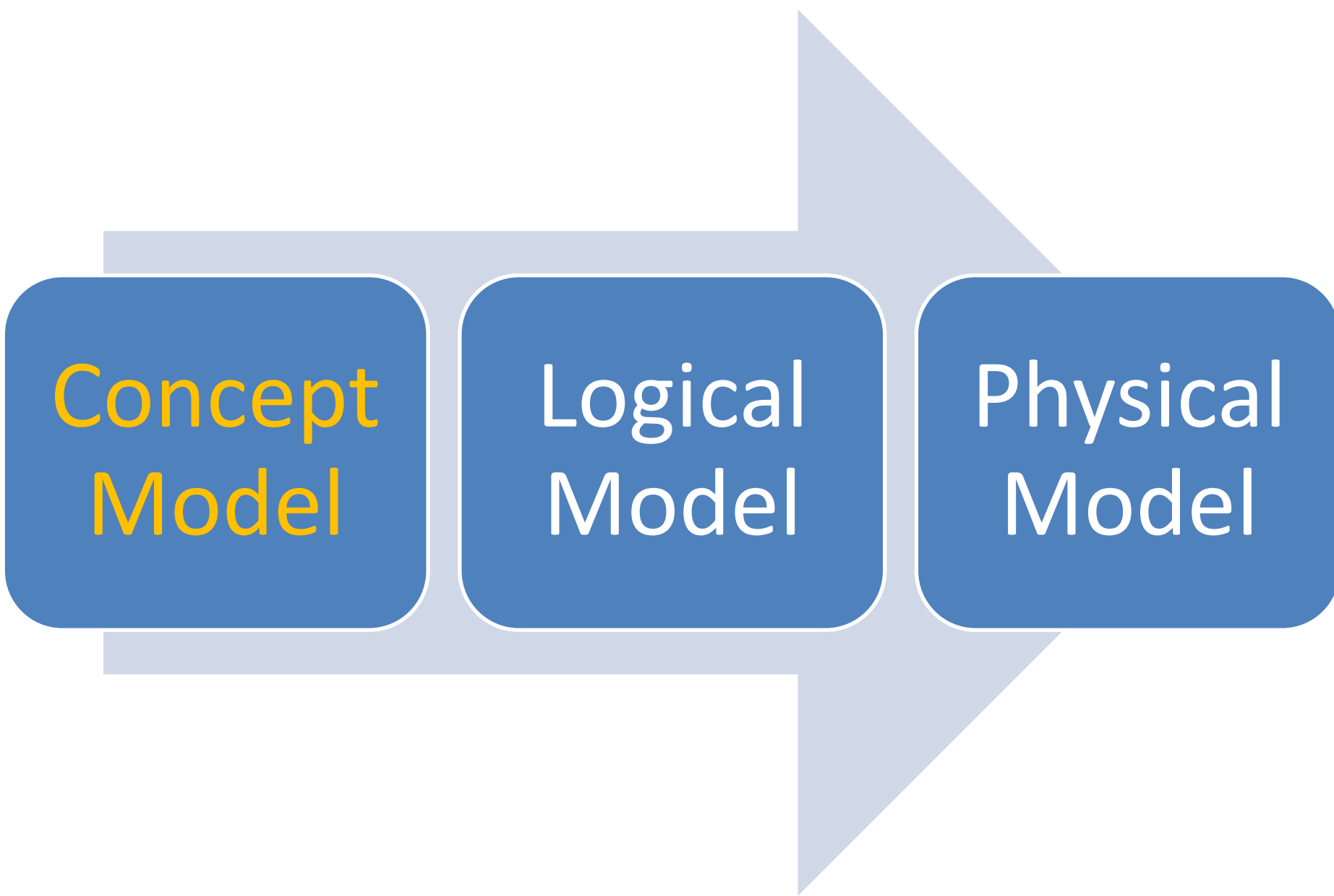


Access Control Models

*Ensuring that the right people have access to the right resources
In compliance with applicable policy*



Gerry Gebel, M. N. (2009). User Authorization. *Burton Group: Identity and Privacy Strategy*



Concept
Model

Logical
Model

Physical
Model

Why Concept Modeling?

Captures Information Requirements



Problem Specific & Technology-neutral

Why Concept Modeling?

Semantic Alignment



Identifies Business Terms
Establishes Semantic Agreement

Why Concept Modeling?

Framework



Conceptual Foundation

Why Concept Modeling?

Agility



Baselines Technology Insertion

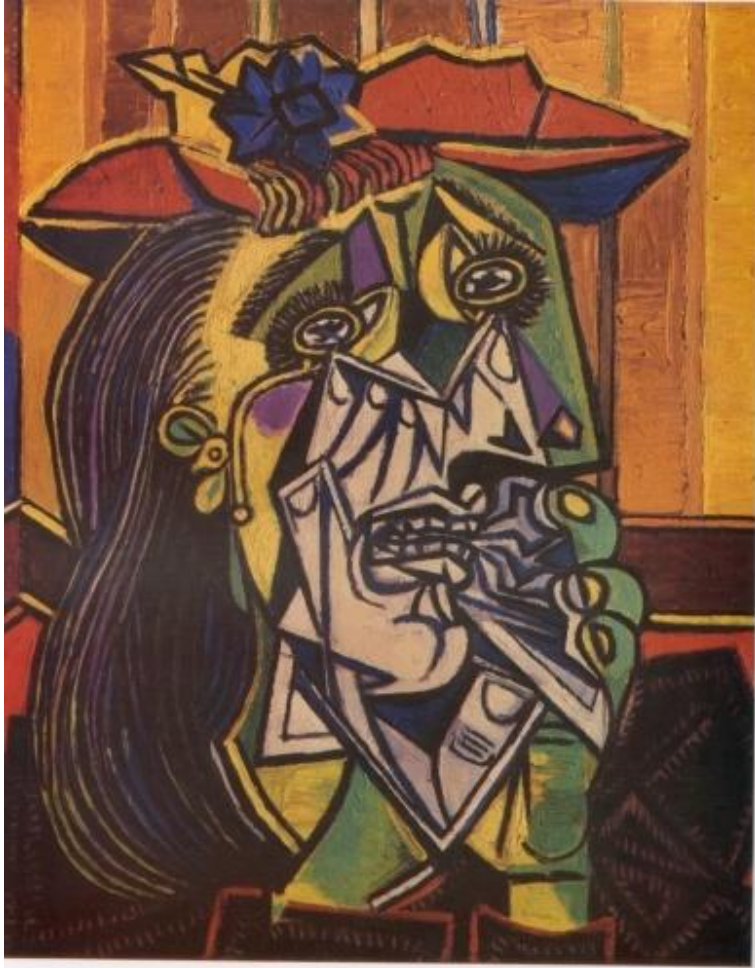
What is a Federal User?

Desired View



What is a Federal User?

Current View

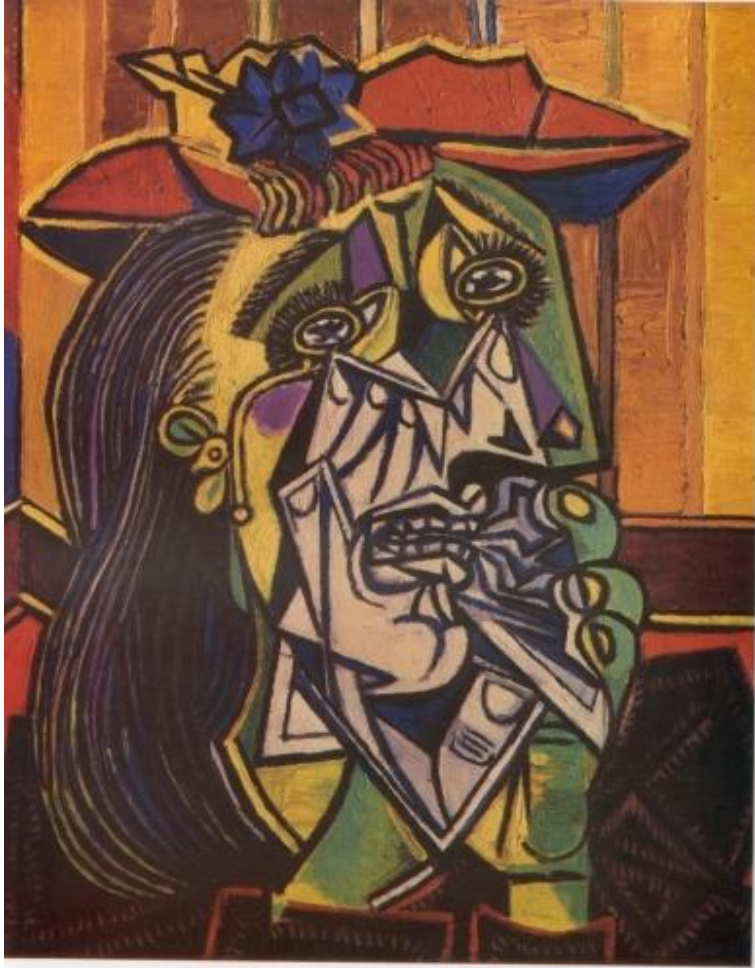


Desired View



What is a Federal User?

Current View

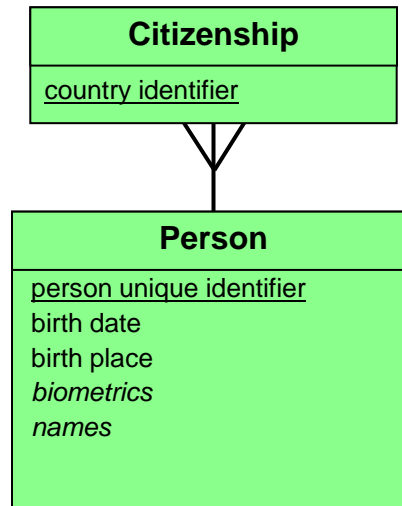


Desired View



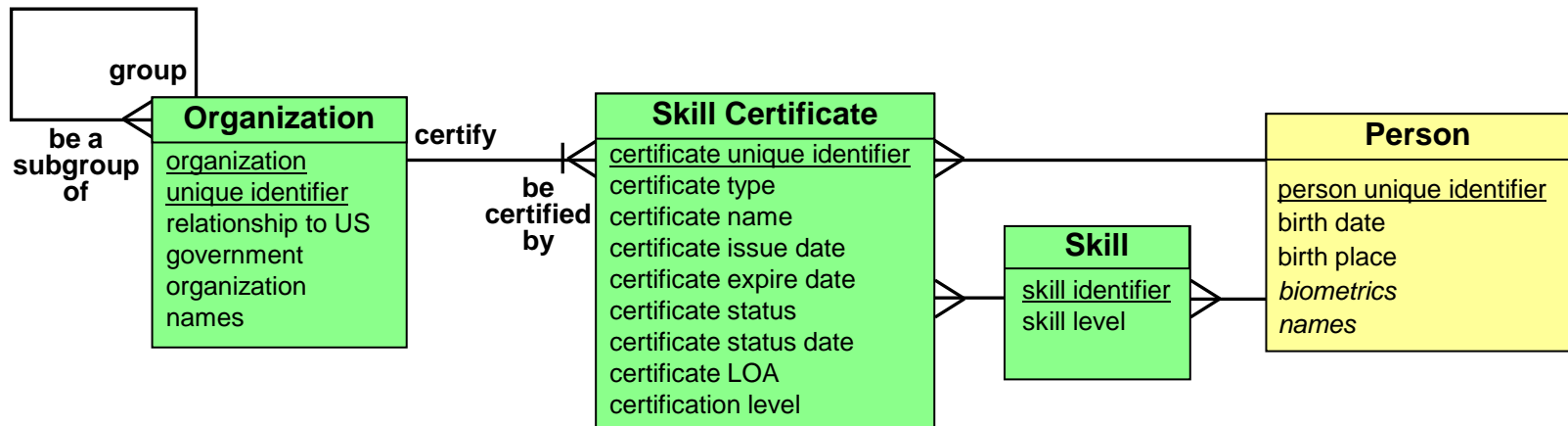
ICAM User Concept Model

I.



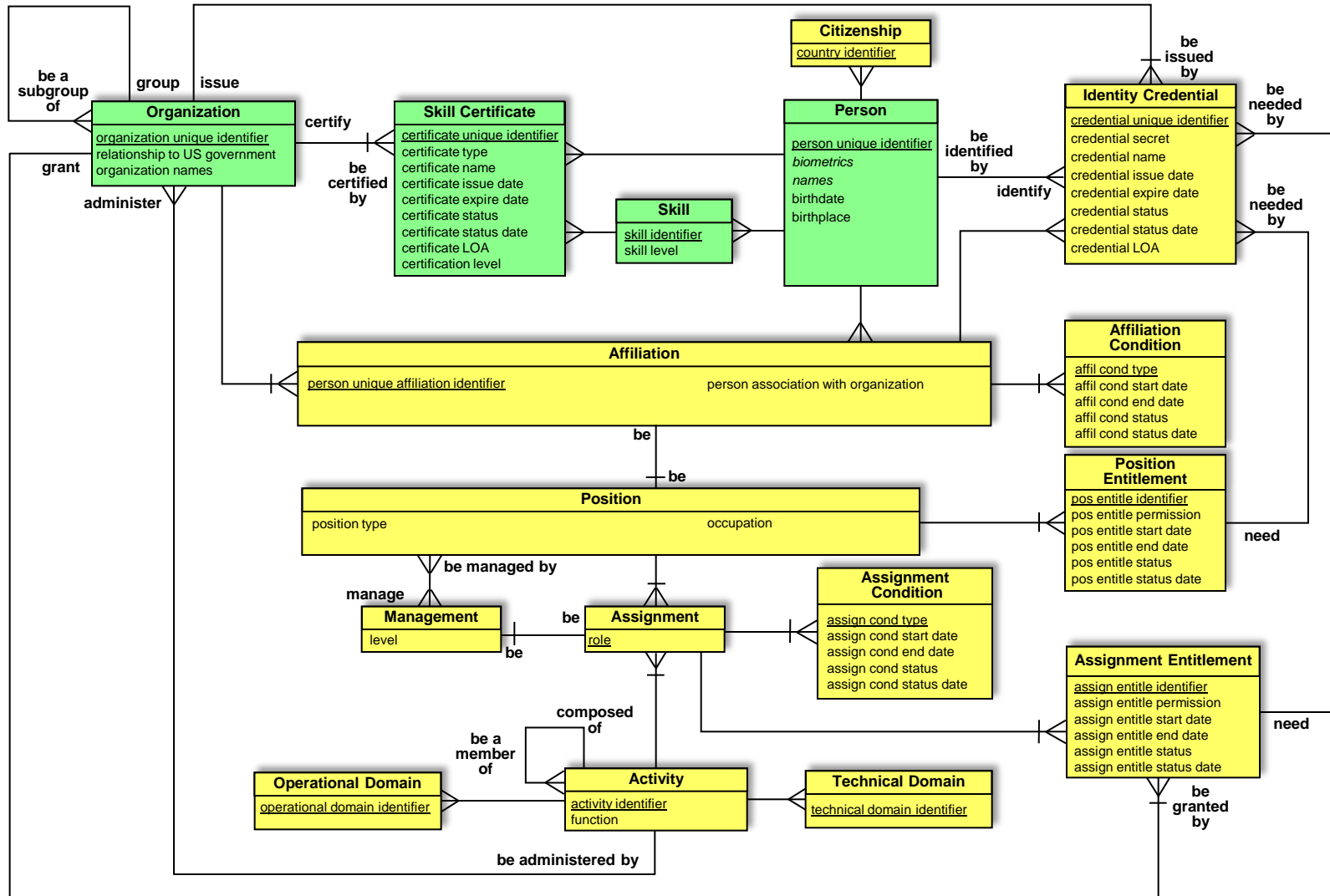
ICAM User Concept Model

II.



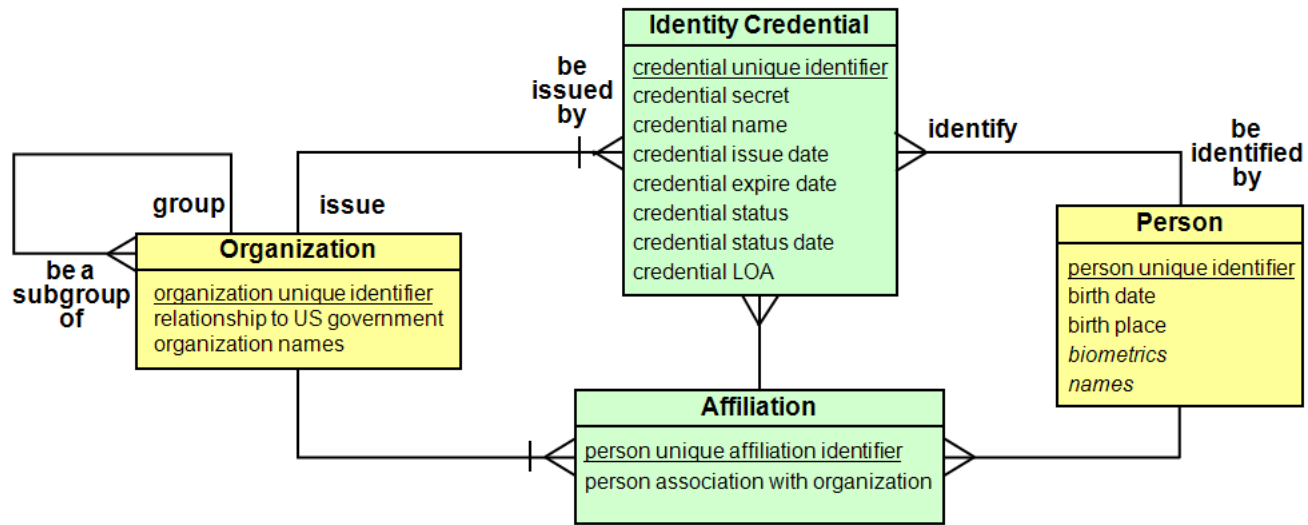
ICAM User Concept Model

II.



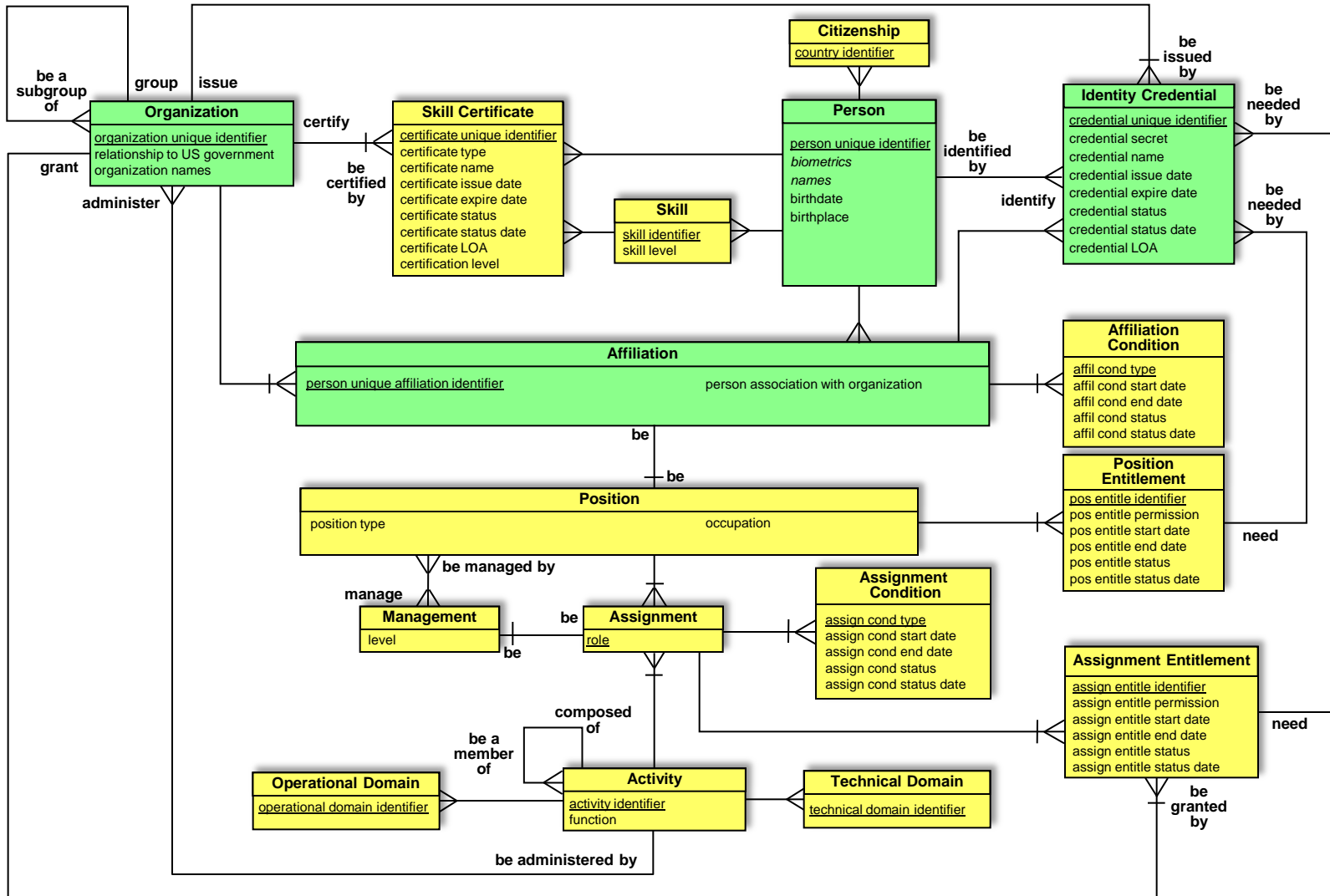
ICAM User Concept Model

III.



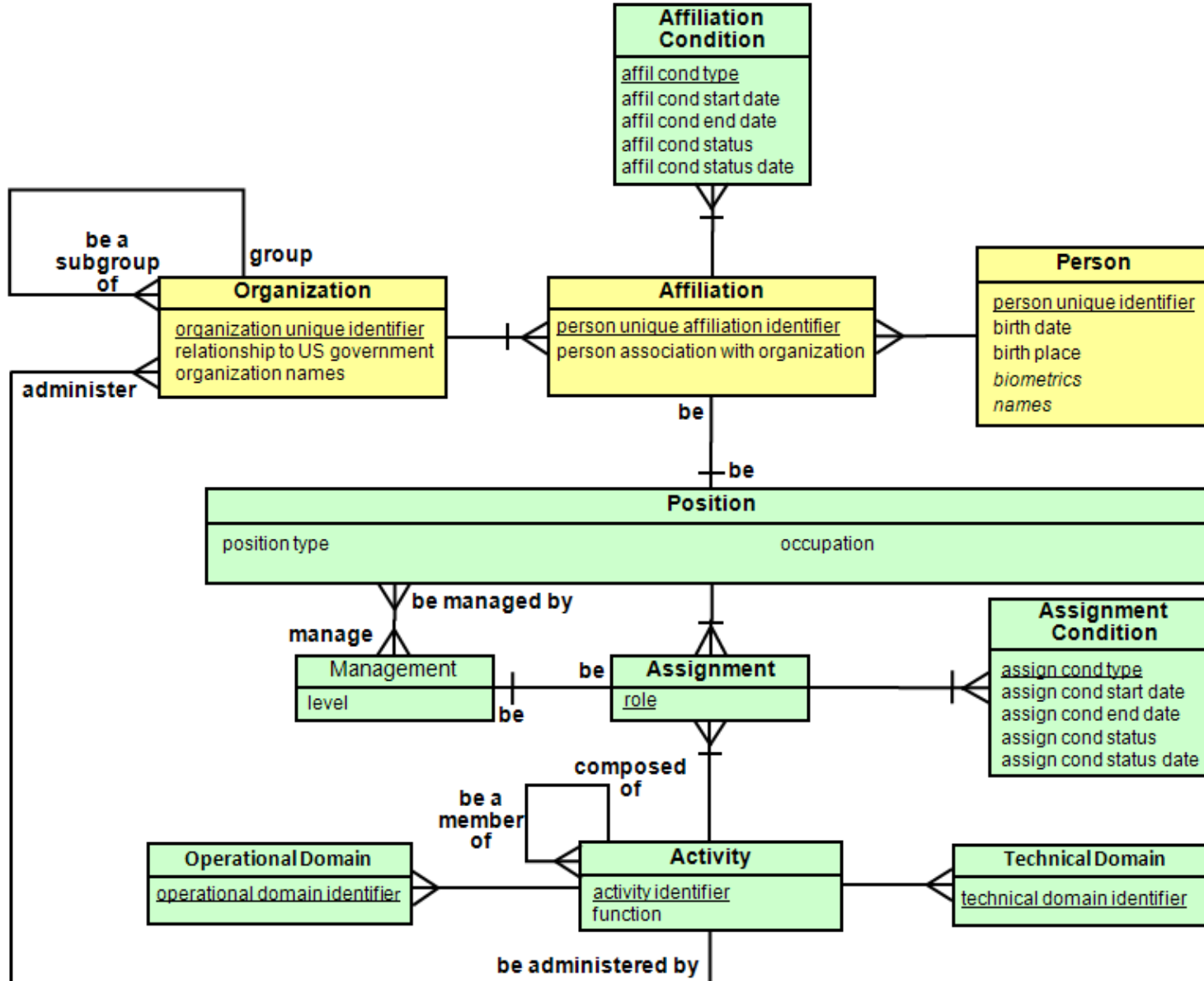
ICAM User Concept Model

III.



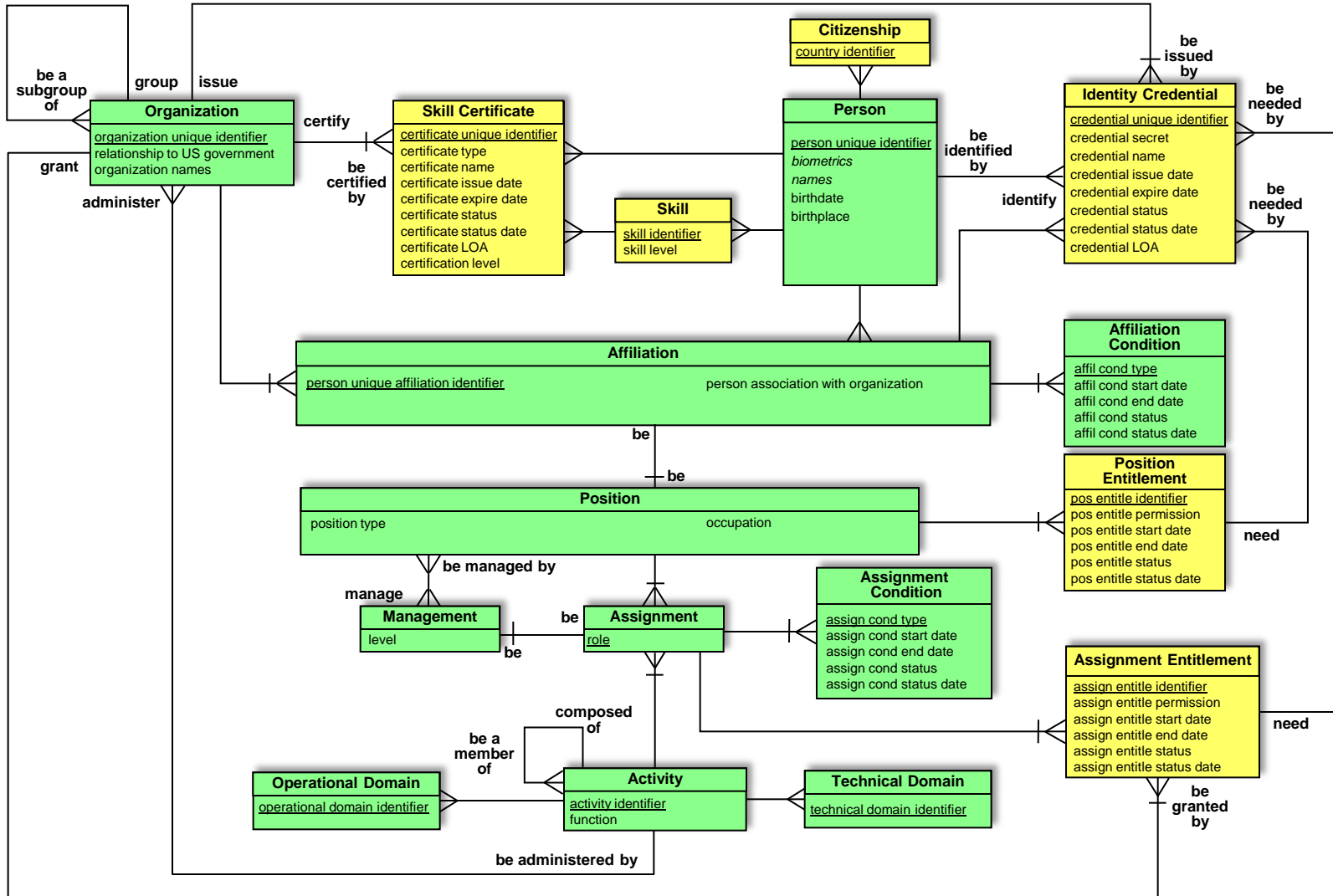
ICAM User Concept Model

IV.



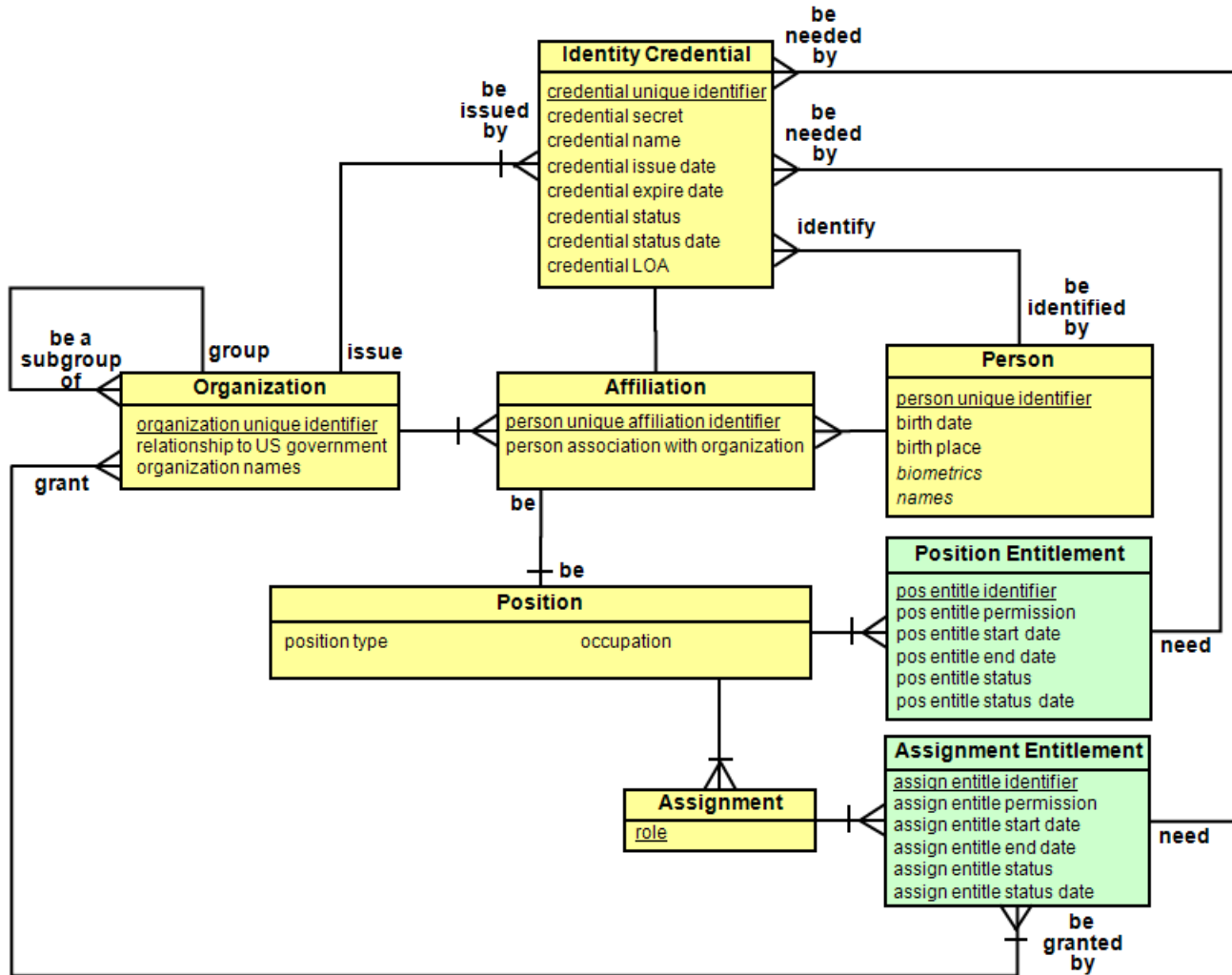
ICAM User Concept Model

IV.



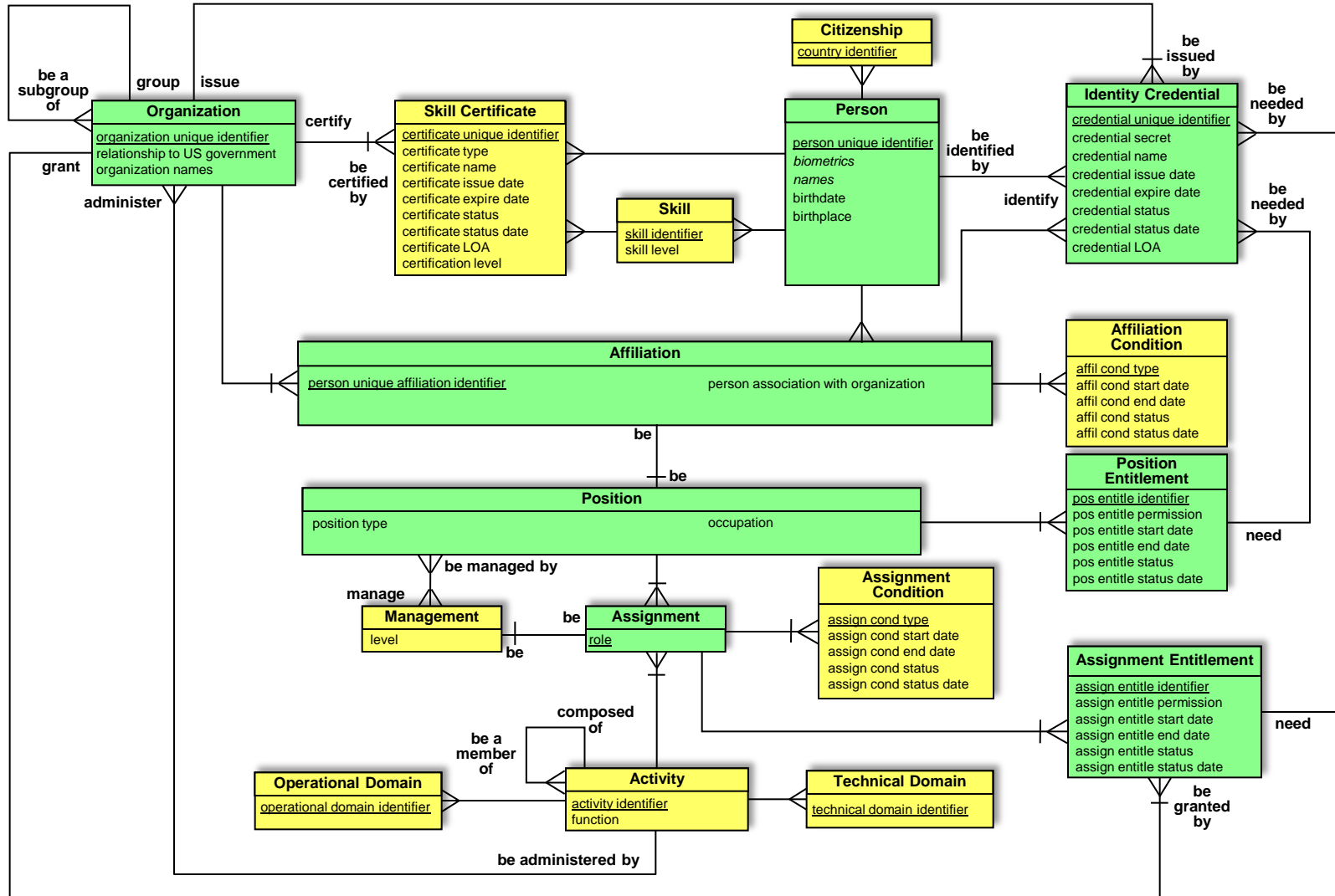
ICAM User Concept Model

V.

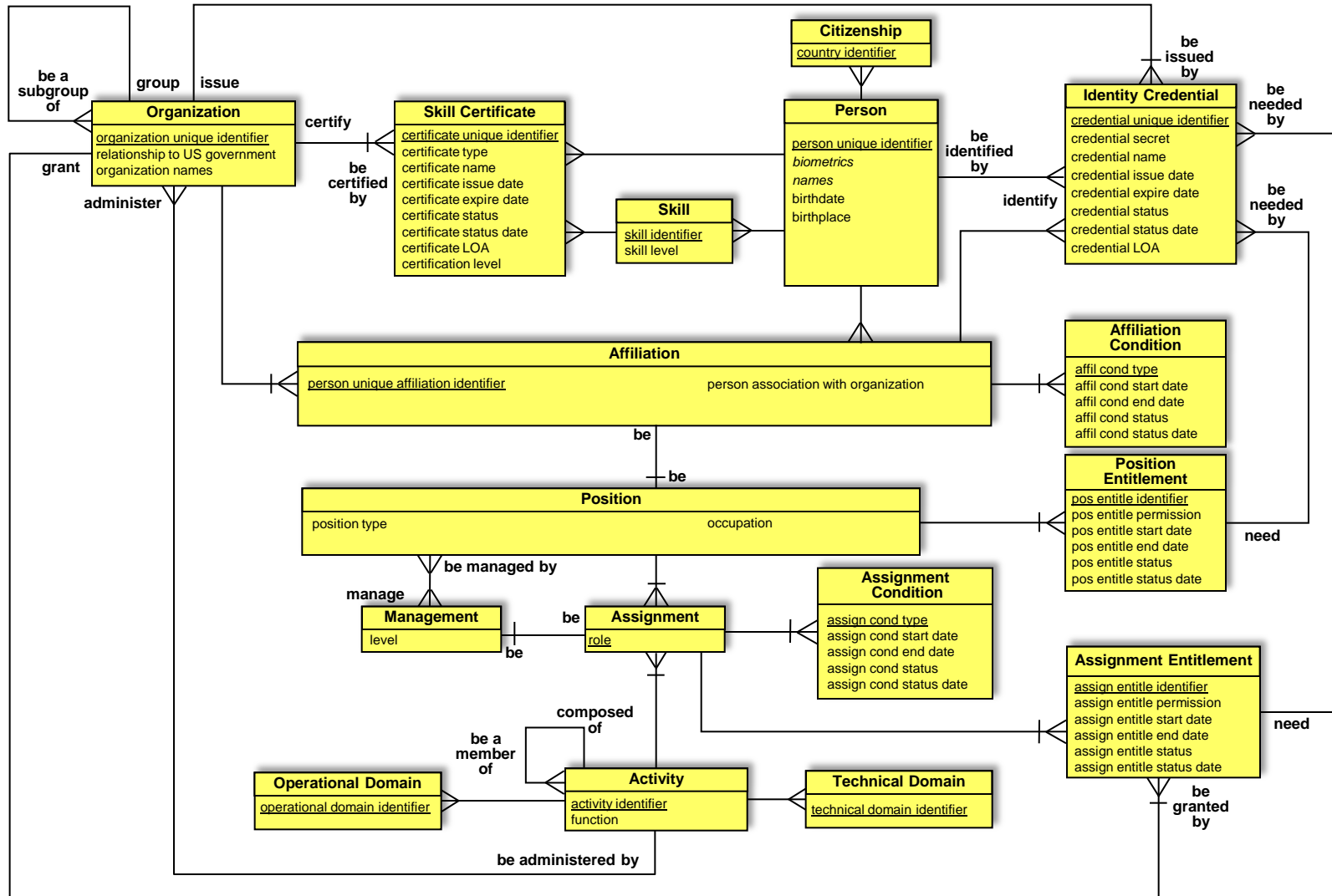


ICAM User Concept Model

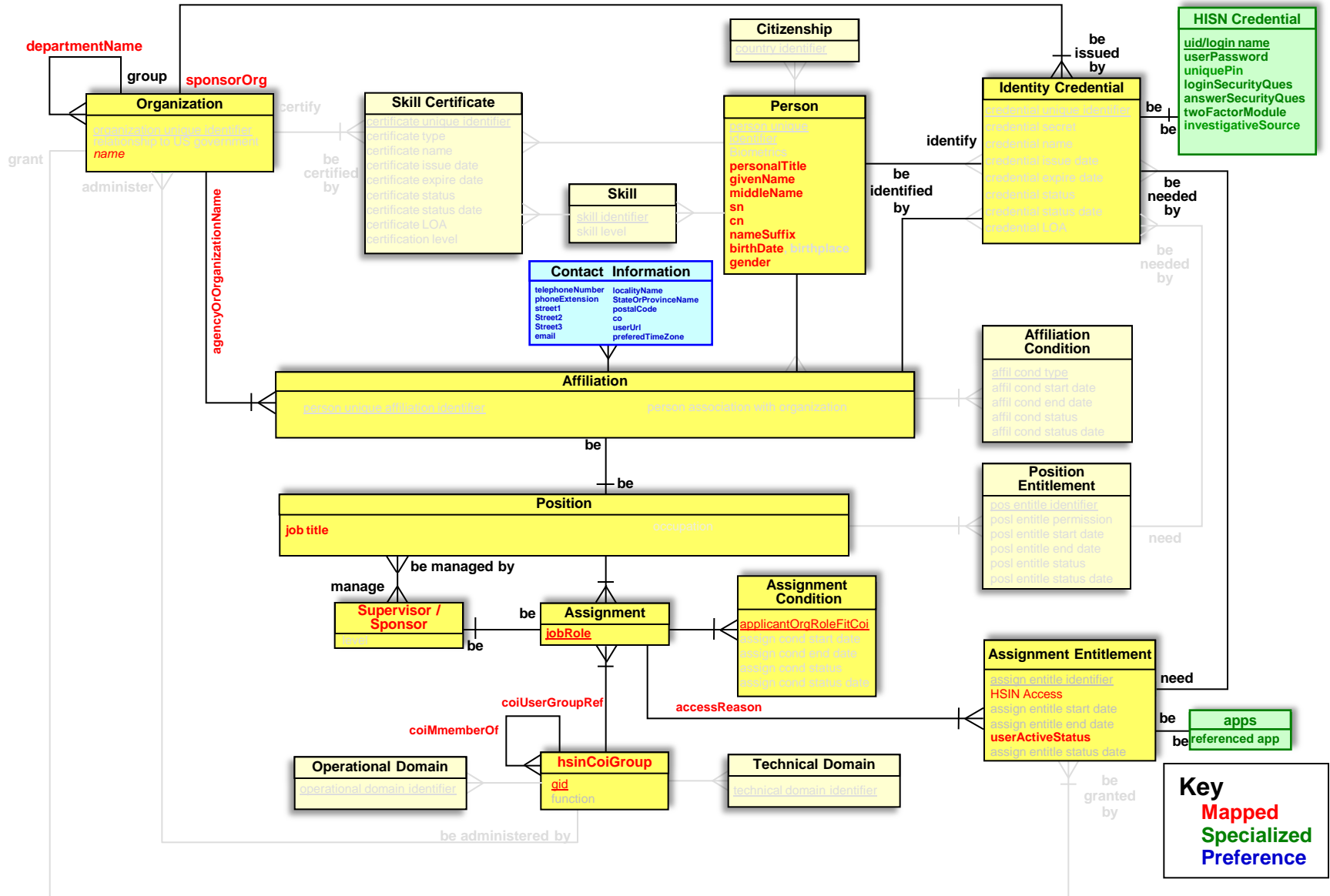
V.



ICAM User Concept Model

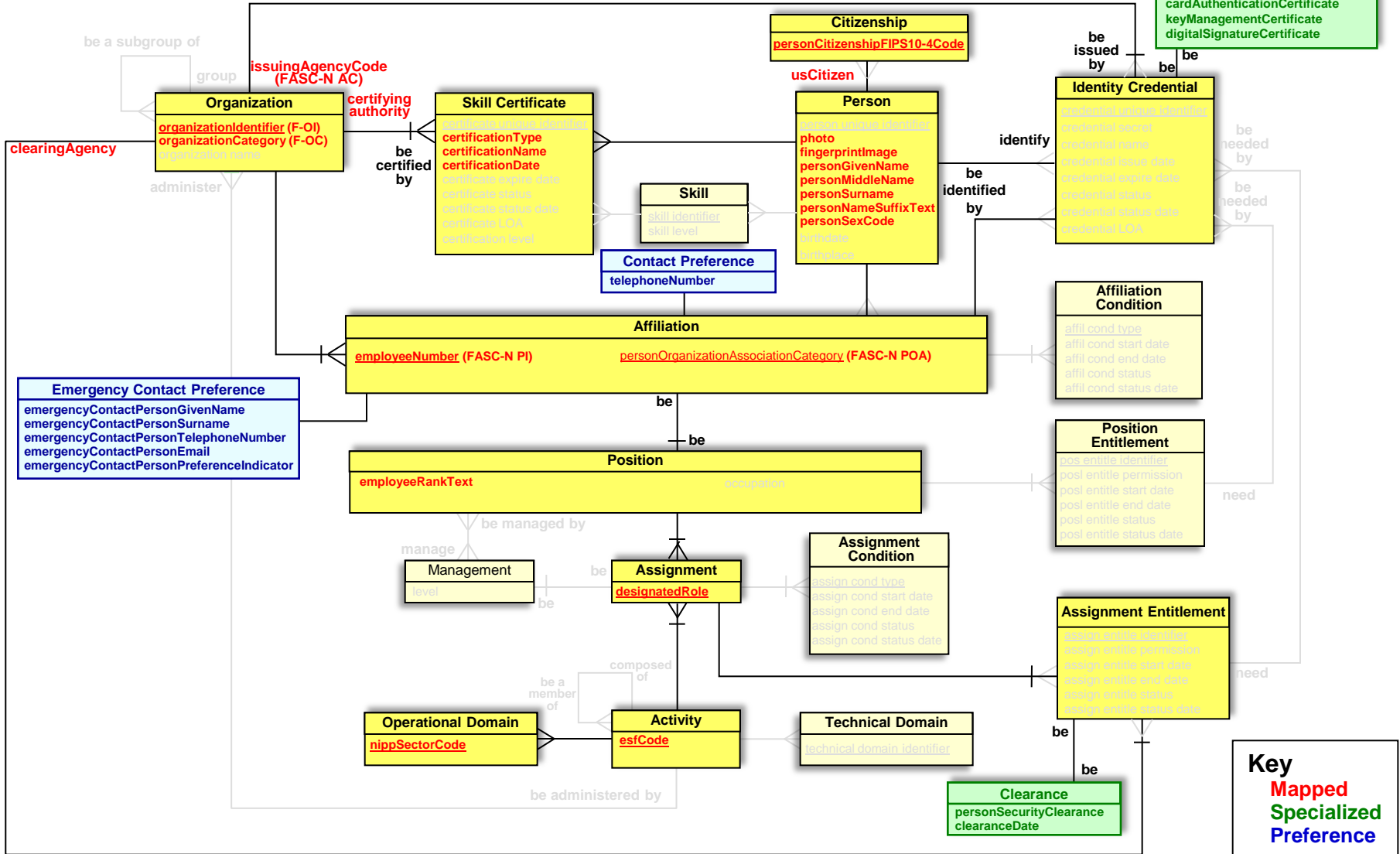


DHS HSIN 2010 Mapping



Federal ICAM BAE v1 Mapping

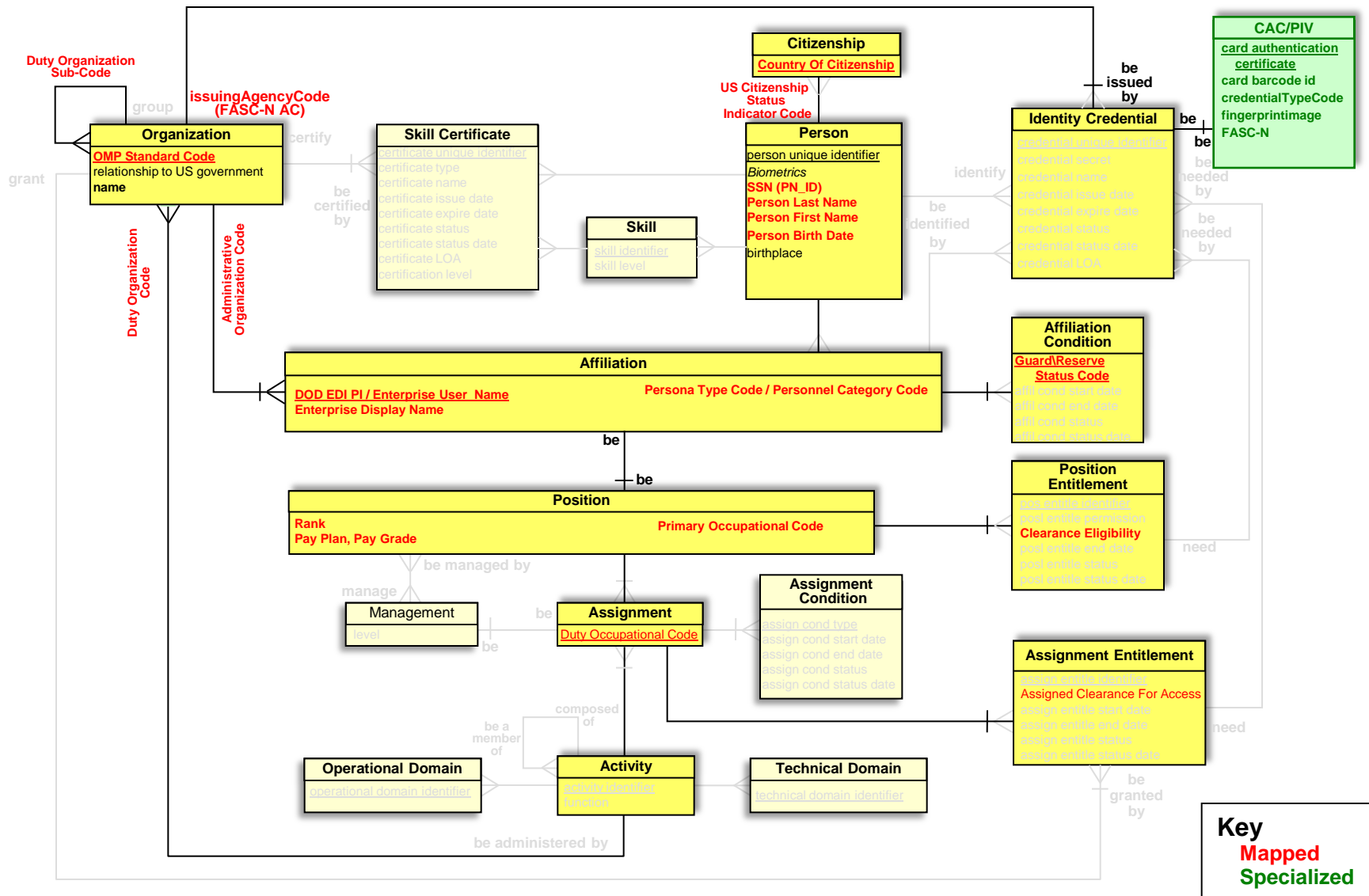
PIV Card
chuid
cardIssueDate
cardExpirationDate
cardStatus
cardStatusDate
chuidStatus
chuidStatusDate
issuedID (FASC-N CN)
IssuingSystemCode (FASC-N SC)
issuedSeries (FASC-N CS)
issuedCredentialCode (FASC-N ICI)
cardAuthenticationCertificate
keyManagementCertificate
digitalSignatureCertificate



Key
Mapped
Specialized
Preference

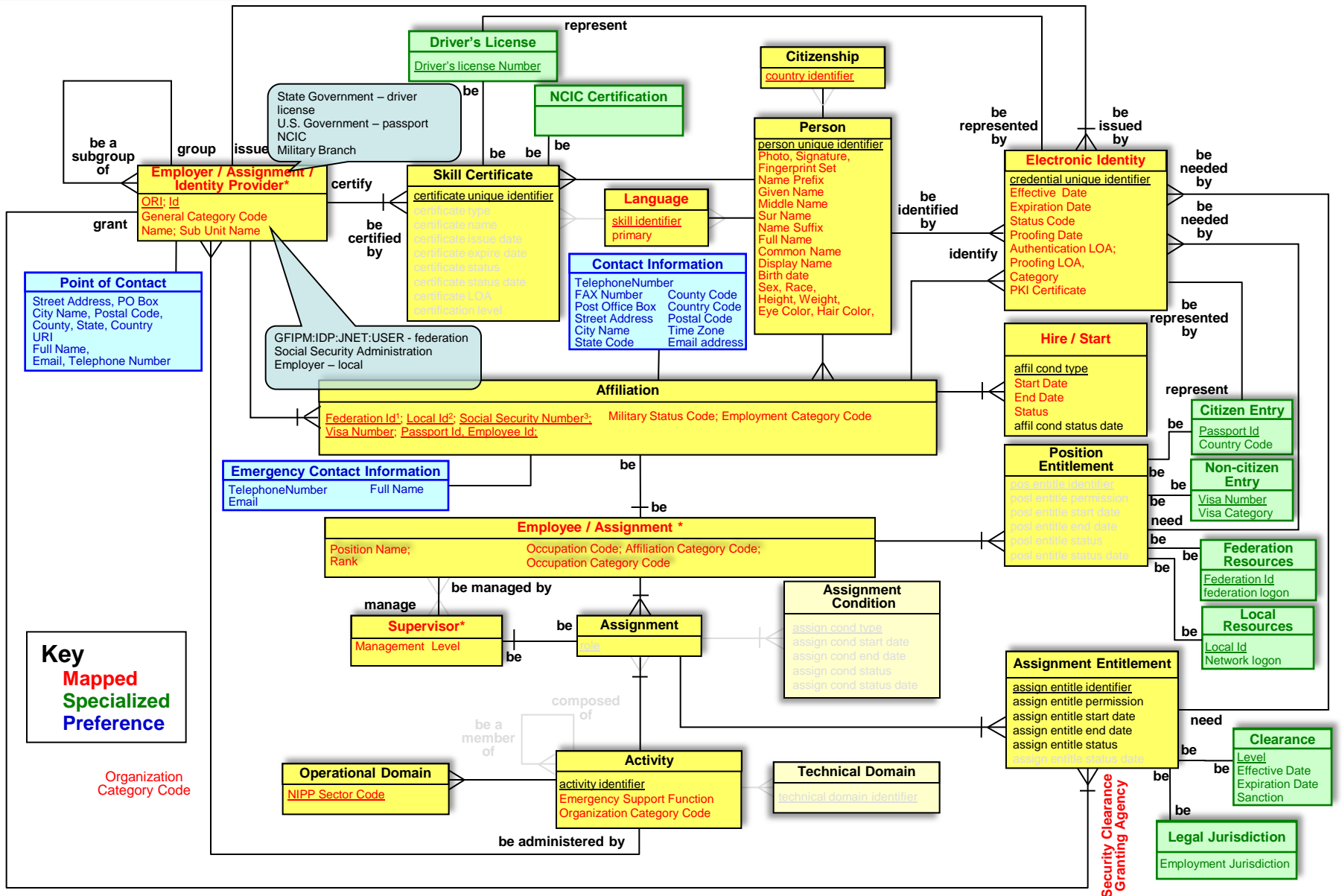
DOD DMDC EAS Mapping

DRAFT



DRAFT

GFIPM V2 Concept Model



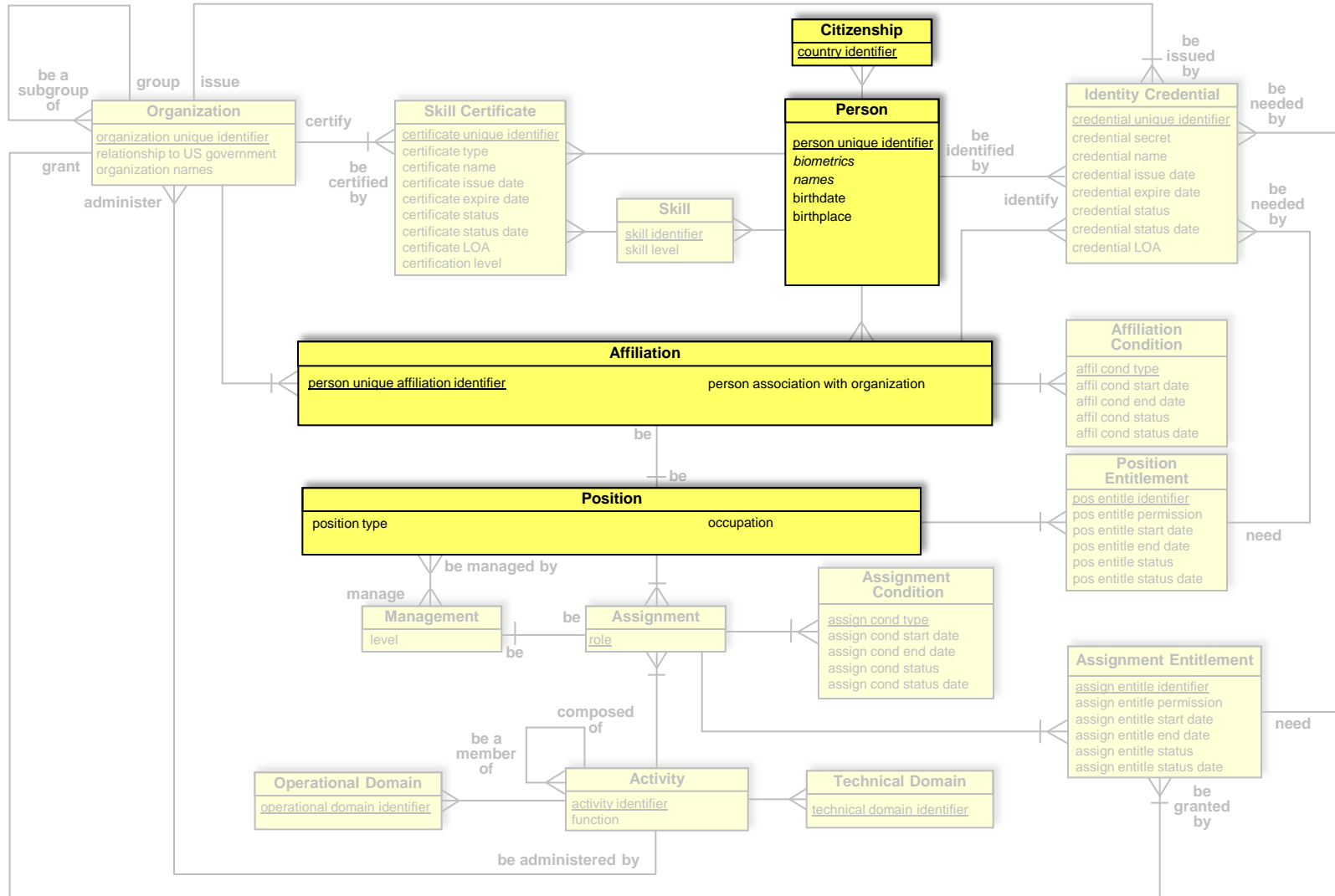
Concept
Model

Logical
Model

Physical
Model

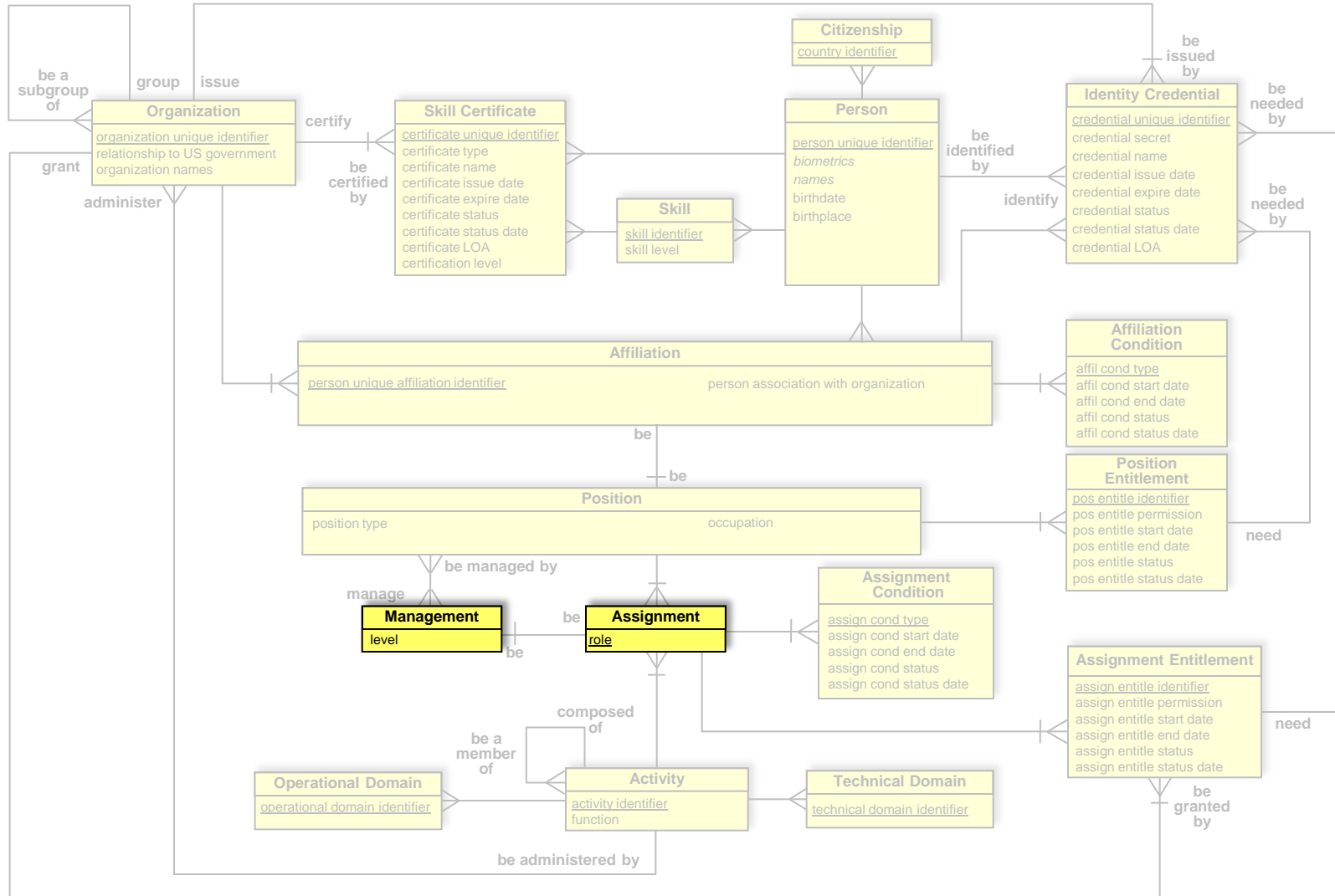
Proposed FICAM User LDAP Model

abacPerson \leftarrow *inetOrgPerson*



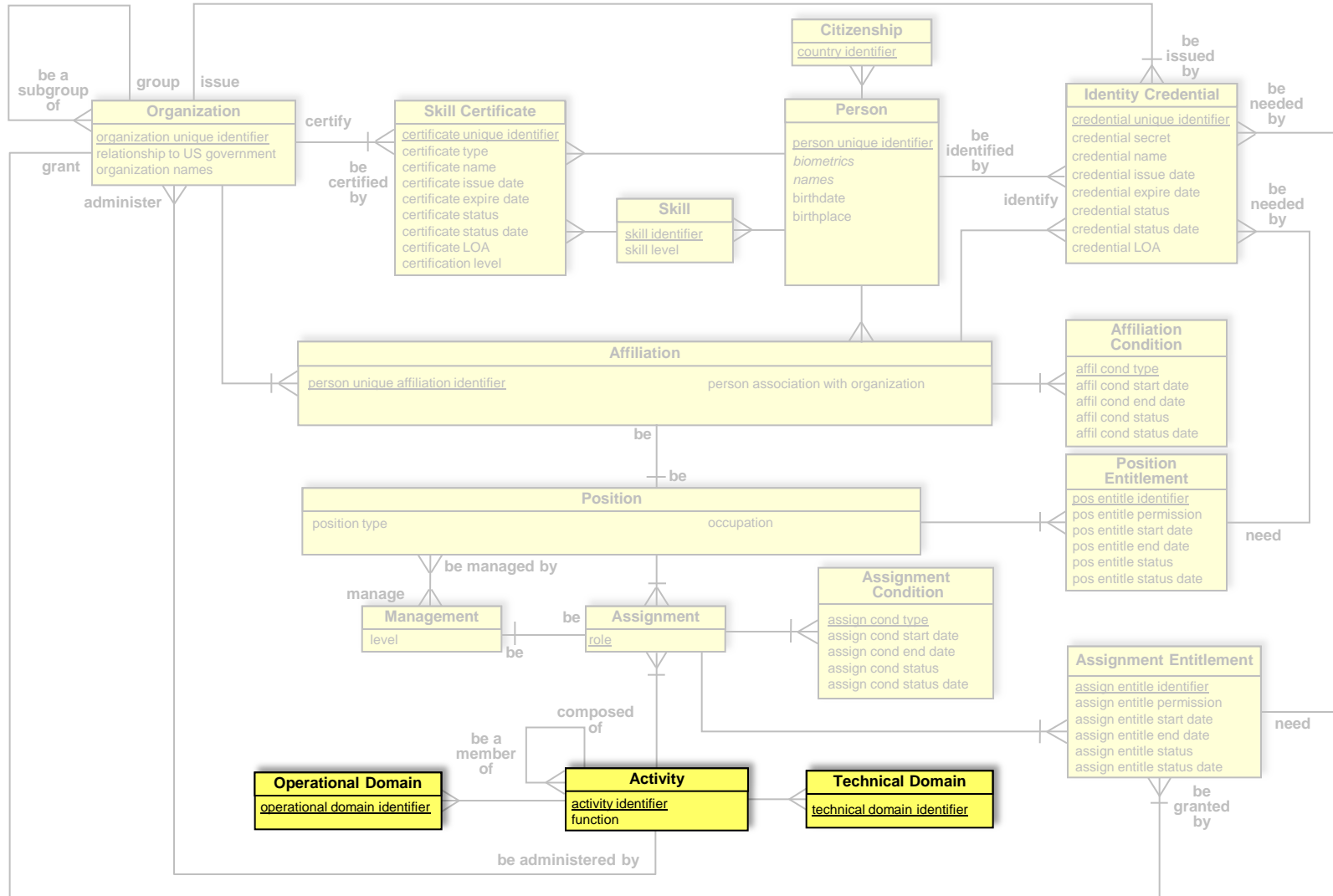
Proposed FICAM User LDAP Model

abacAssignment



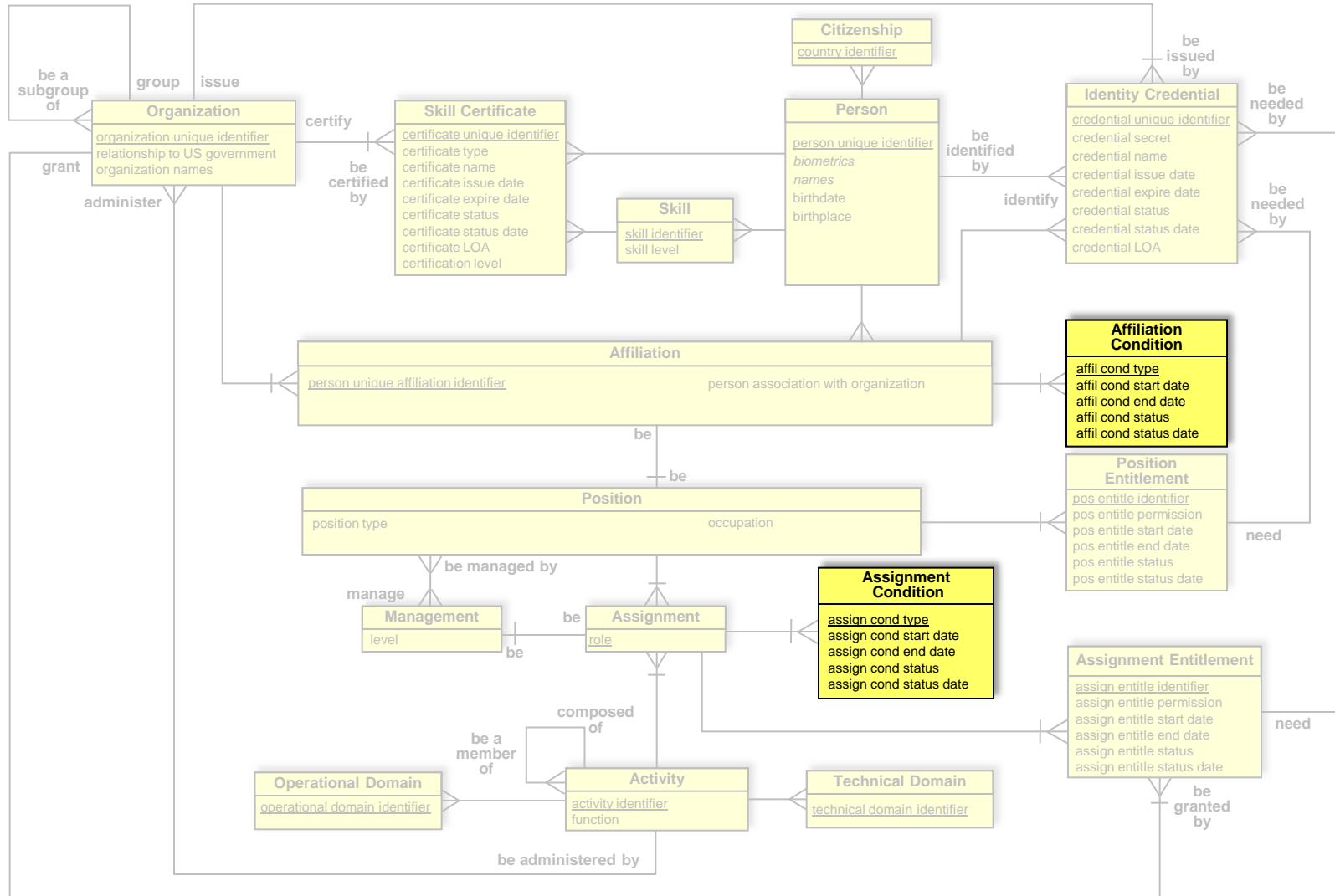
Proposed FICAM User LDAP Model

abacActivity <= *groupOfUniqueNames*



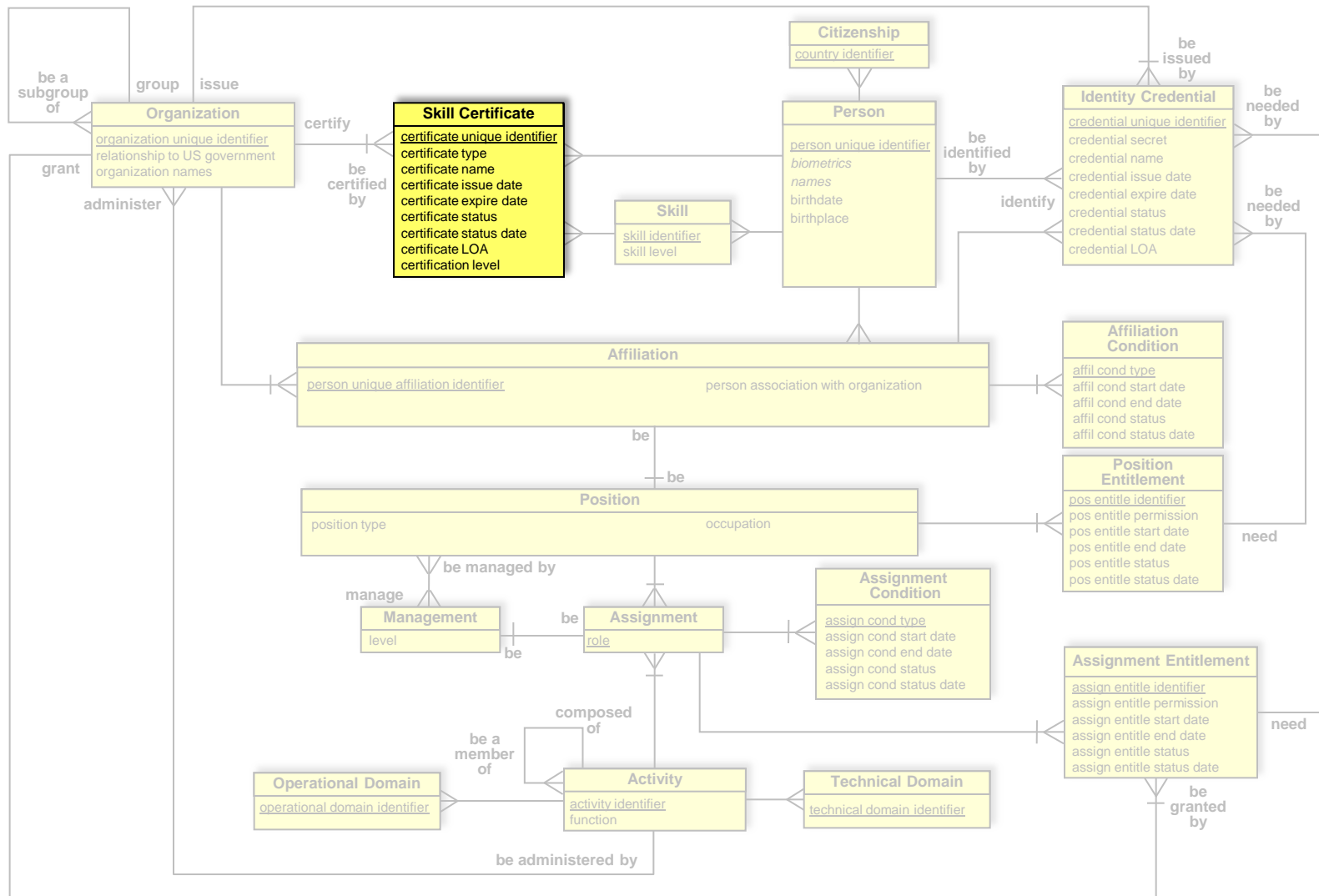
Proposed FICAM User LDAP Model

abacCondition



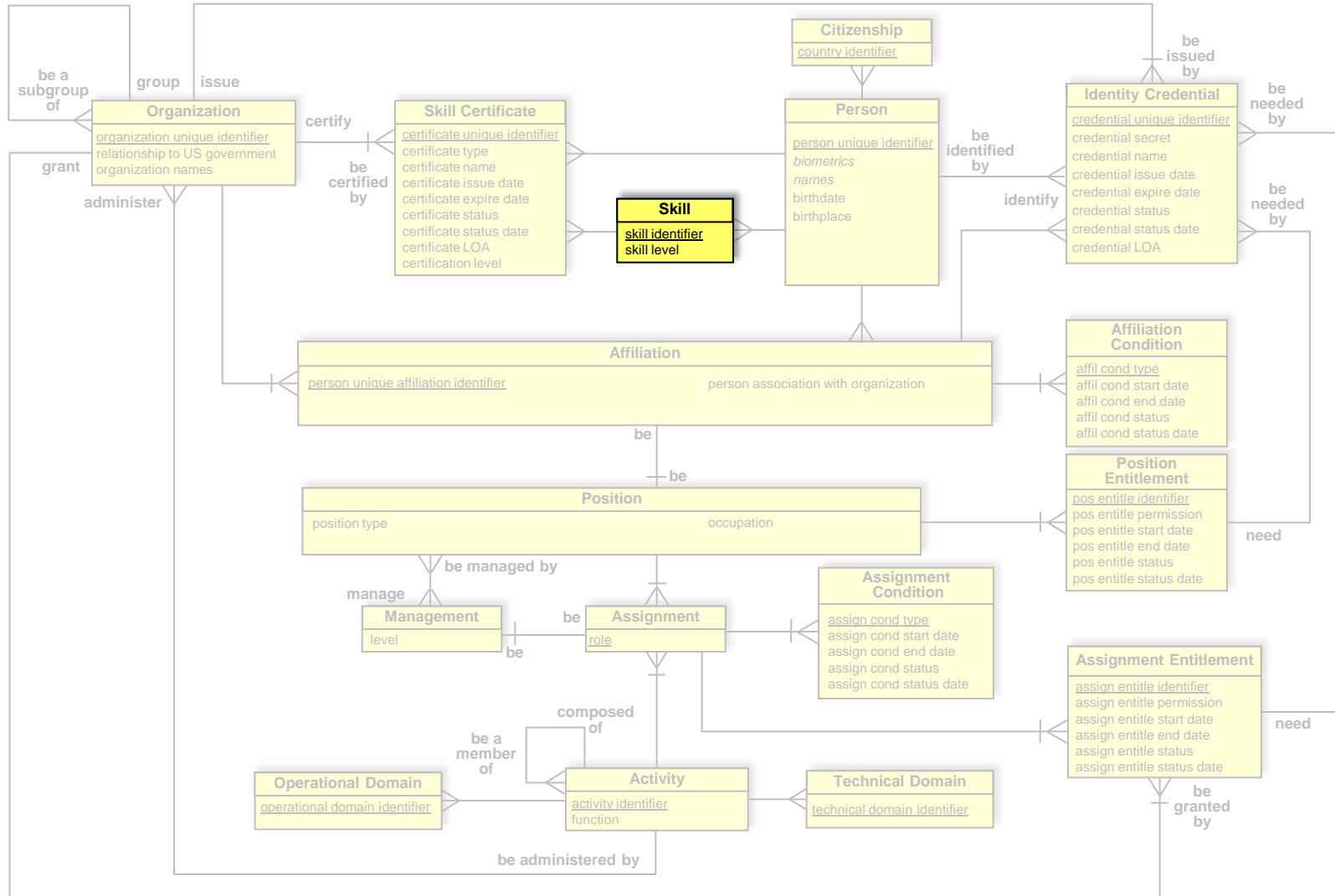
Proposed FICAM User LDAP Model

abacCertification

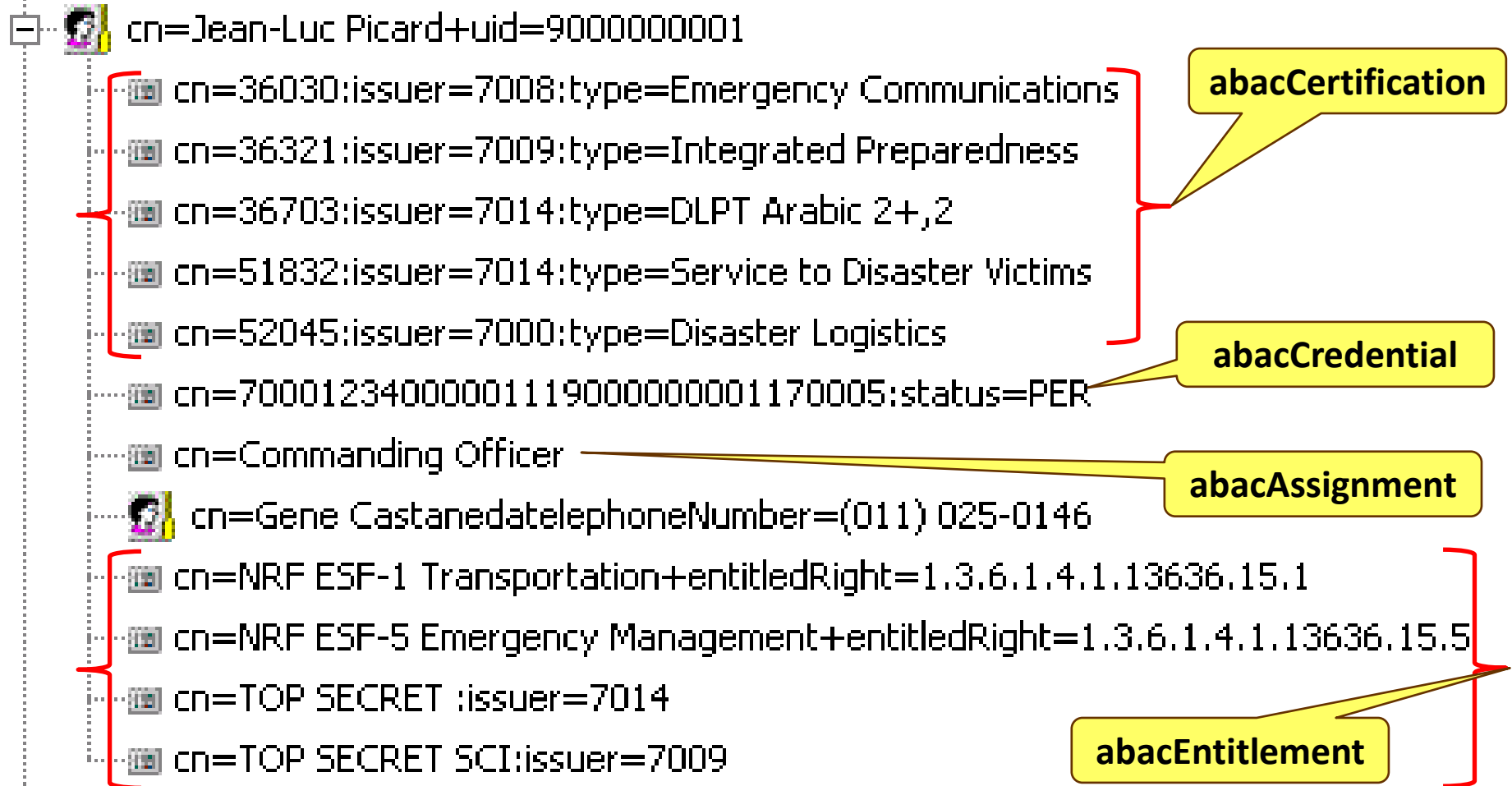


Proposed FICAM User LDAP Model

abacSkill



abacPerson Objects

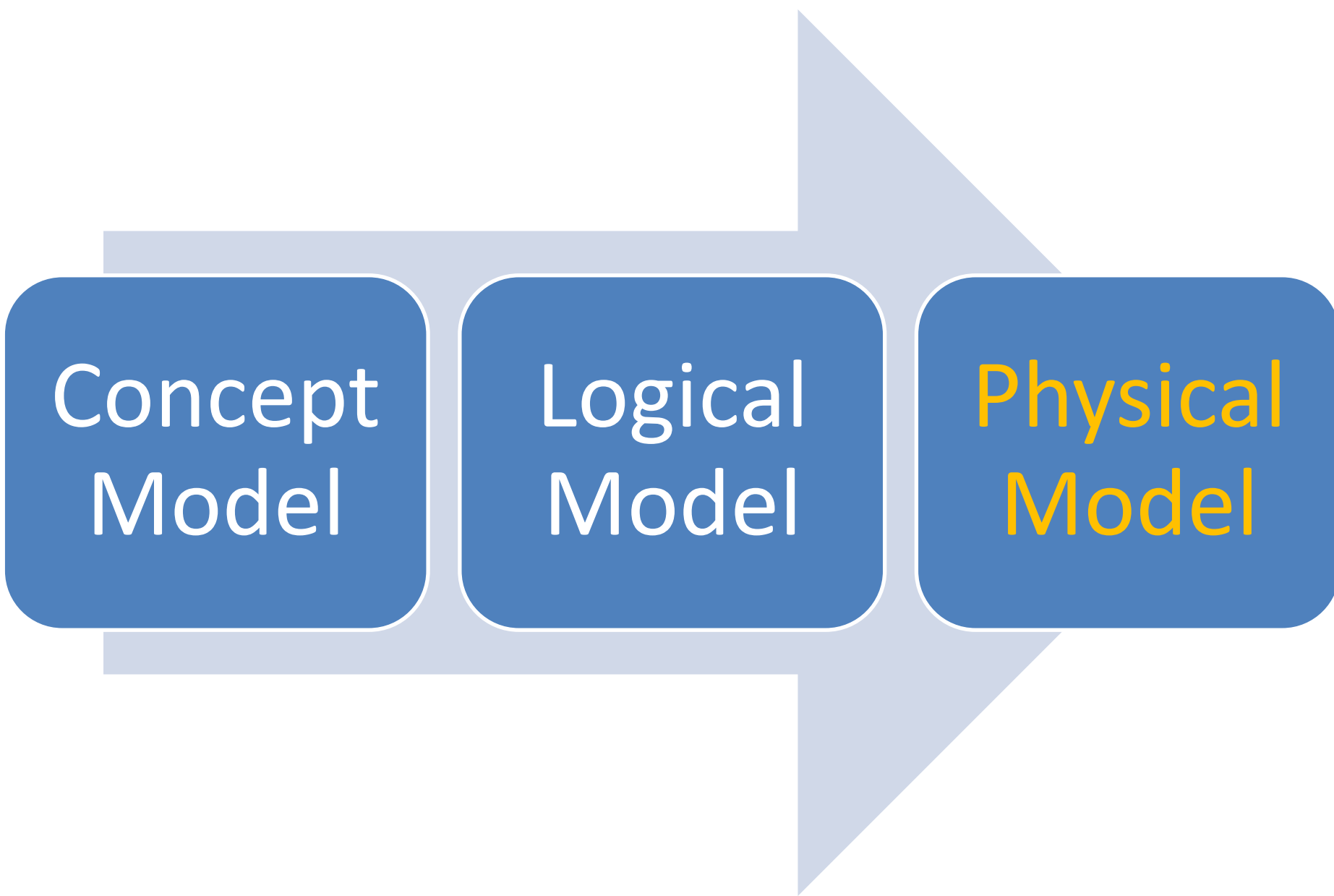


abacPerson Objects

employeeHireDate	2002-09-09
certification	cn=36321:issuer=7009:type=Integrated Preparedness
certification	cn=36030:issuer=7008:type=Emergency Communications
certification	cn=36703:issuer=7014:type=DLPT Arabic 2+,2
certification	cn=52045:issuer=7000:type=Disaster Logistics
certification	cn=51832:issuer=7014:type=Service to Disaster Victims
objectclass	top
objectclass	vdapcontainer
objectclass	person
objectclass	organizationalPerson
objectclass	inetorgperson
objectclass	abacPerson
sn	Picard
employeeRank	Captain

abacPerson Objects

title	Commanding Officer
givenName	Jean-Luc
citizenship	FR
o	Starfleet
middleName	
l	Dayton
entitlement	cn=TOP SECRET SCI:issuer=7009
entitlement	cn=NRF ESF-1 Transportation+entitledRight=1.3.6.1.4.1.13636.15.1
entitlement	cn=NRF ESF-5 Emergency Management+entitledRight=1.3.6.1.4.1.13636.15.5
entitlement	cn=TOP SECRET :issuer=7014
employeeStatus	ACTIVE
gender	M
credential	cn=70001234000001119000000001170005:status=PER



Concept
Model

Logical
Model

Physical
Model

BAE v2 Attribute Request

```
<soapenv:Envelope xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Header>
</soapenv:Header>
  <soapenv:Body>
    <samlp:AttributeQuery Destination="URN:TEST:IDMANAGEMENT.GOV:ICAM:BAE:V2:STARFLEET" ID="_soapui${=(int)(Math.random()*1000000)}" IssueInstant="{ZuluTime}" Version="2.0">
      <saml:Issuer>URN:TEST:IDMANAGEMENT.GOV:ICAM:BAE:V2:EARTH</saml:Issuer>
      <saml:Subject>
        <saml:NameID Format="urn:idmanagement.gov:icam:bae:v2:SAML:2.0:nameid-format:fasn">70001234000001119000000001170005</saml:NameID>
      </saml:Subject>
    </samlp:AttributeQuery>
  </soapenv:Body>
</soapenv:Envelope>
```

BAE v2 Attribute Response

```
<saml2:AttributeStatement>
  <saml2:Attribute Name="urn:test:idmanagement.gov:icam:attribute:v1:mail" NameFormat=
    "urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml2:AttributeValue>JeanLuc.Picard@test.dhs.gov</saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute Name="urn:test:idmanagement.gov:icam:attribute:v1:sn" NameFormat=
    "urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml2:AttributeValue>Picard</saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute Name="urn:test:idmanagement.gov:icam:attribute:v1:organizationName" NameFormat=
    "urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml2:AttributeValue>Starfleet</saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute Name="urn:test:idmanagement.gov:icam:attribute:v1:ESFcode" NameFormat=
    "urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml2:AttributeValue>1.3.6.1.4.1.13636.15.5</saml2:AttributeValue>
    <saml2:AttributeValue>1.3.6.1.4.1.13636.15.15</saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute Name="urn:test:idmanagement.gov:icam:attribute:v1:organizationUnitName" NameFormat=
    "urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml2:AttributeValue>Command Staff</saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute Name="urn:test:idmanagement.gov:icam:attribute:v1:designatedRole" NameFormat=
    "urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml2:AttributeValue>Commanding Officer</saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute Name="urn:test:idmanagement.gov:icam:attribute:v1:givenName" NameFormat=
    "urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml2:AttributeValue>Jean-Luc</saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute Name="urn:test:idmanagement.gov:icam:attribute:v1:facsc-n" NameFormat=
    "urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml2:AttributeValue>70001234000001119000000001170005</saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute Name="urn:test:idmanagement.gov:icam:attribute:v1:countryOfCitizenship" NameFormat=
    "urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml2:AttributeValue>FR</saml2:AttributeValue>
  </saml2:Attribute>
</saml2:AttributeStatement>
```

Questions?

Contact Information

- **Karyn Higa-Smith (DHS S&T)**
 - Program Manager, Identity Management
 - Karyn.Higa-Smith@dhs.gov
- **Thomas Smith (JHU/APL)**
 - Senior Engineer, DHS S&T IdM Testbed
 - Thomas.Smith@jhuapl.edu
- **Maria Vachino (JHU/APL)**
 - Senior Engineer, DHS S&T IdM Testbed
 - Maria.Vachino@jhuapl.edu

Backup Slides

Why A Conceptual Data Model?

- **Captures Information Requirements**
 - Problem specific
 - Technology-neutral
 - Information representation, not process or policy
 - Identifies business terms
 - Establishes contextual consensus
 - Expresses data semantics
- **Artifacts**
 - Entities
 - Attributes
 - Relationships
 - Identifiers
 - Problem Terms

Concept Data Model Uses

- **Knowledge management**
 - Framework for technology insertion – logical/physical modeling
 - Establishes conceptual foundation
 - Baselines technological insertion
 - Aligns organizational information perception
 - Identifies important & distinguishing information
 - Establishes artifacts – entities, attributes, relationships, identifiers, problem terms
- **Improve productivity and agility**
 - Semantic consensus
 - Identifies schema translation requirements
 - Starting point for information sharing agreements
 - Authoritative sources
 - Identifies policy information requirements
 - Policy creation & refinement
 - Identifies information valued by the enterprise
 - Identifies policy overlaps and gaps

User Attribute Contract Mappings

- **Reveal**
 - Contract
 - Concept utilization and specialization
 - Policy focus
 - Unused concepts
 - Purpose (AuthN, AuthZ, Security, Preference) coverage
 - Organization and partner
 - Alignment
 - Discrepancies
- **Support**
 - Federation agreements
 - Semantic consensus
 - Policy analysis and development
 - Identify authoritative source requirements