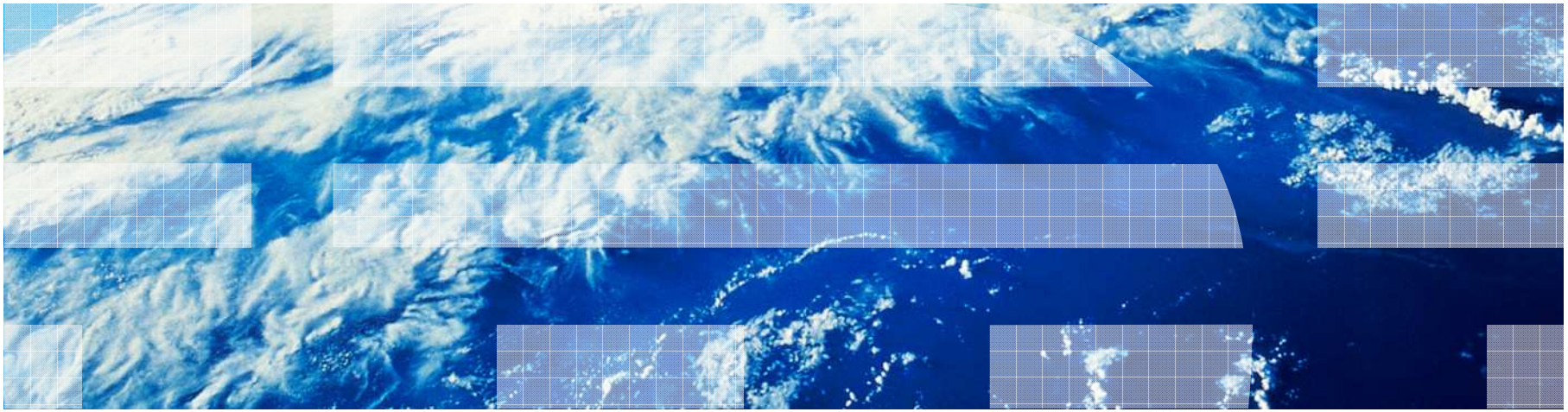
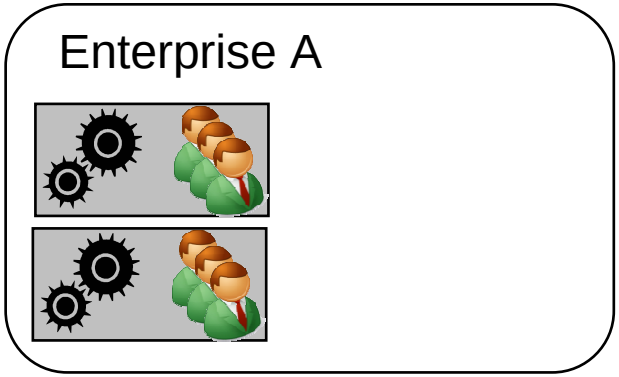
Gregory Neven, IBM Research – Zurich
W3C Workshop on Access Control Scenarios, Nov. 18th, 2009, Luxembourg

Jan Camenisch, Sebastian Mödersheim, Gregory Neven,
Franz-Stefan Preiss, Dieter Sommer

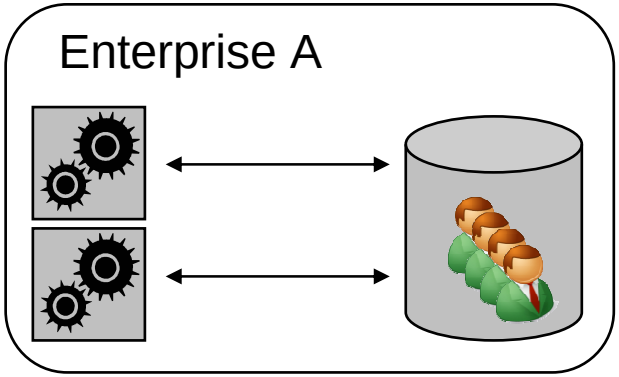
Credential-based access control extensions to XACML

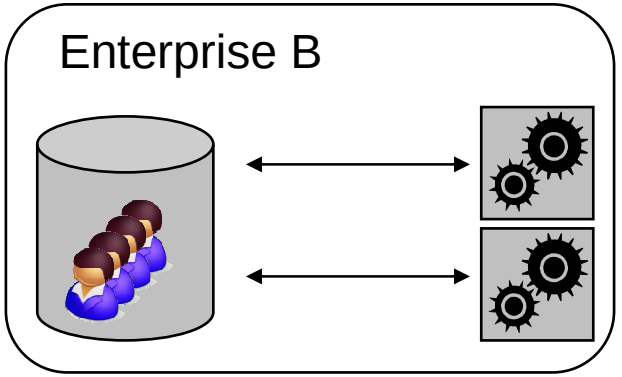


Application identity management

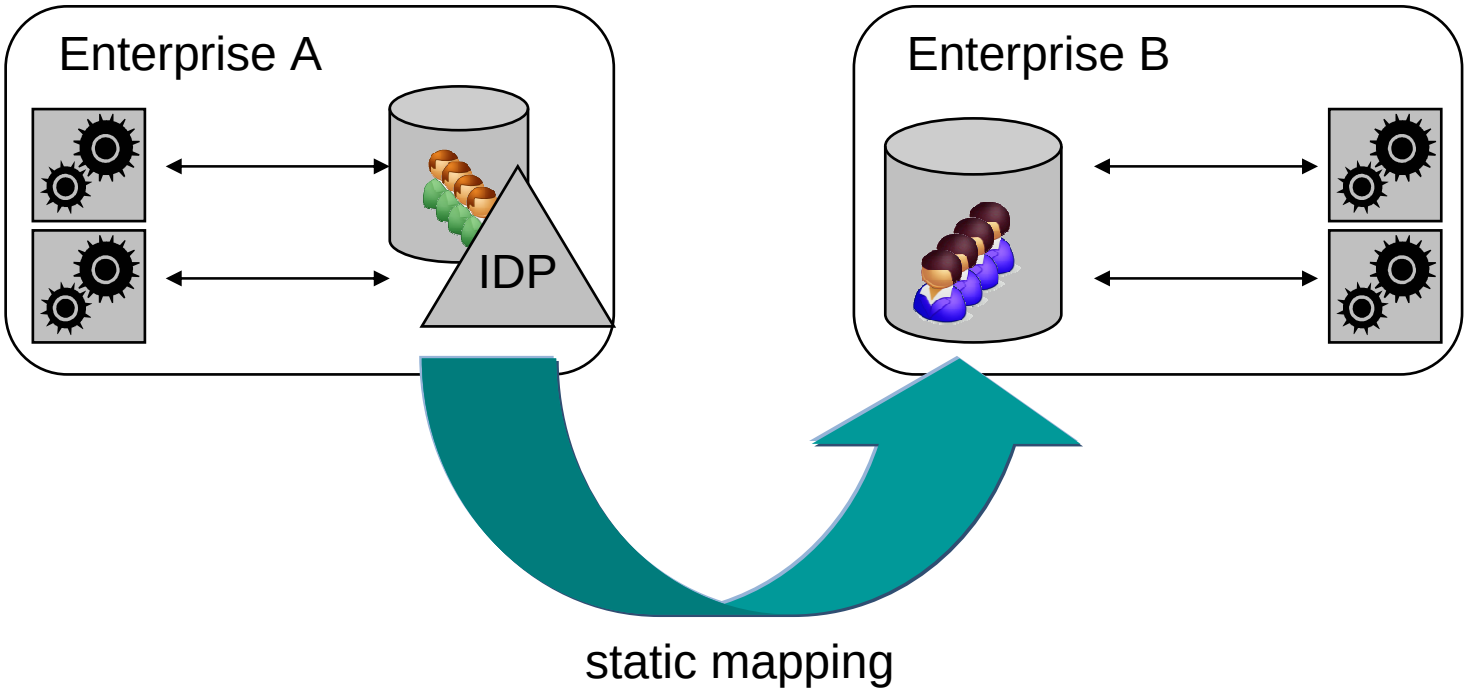


Enterprise identity management

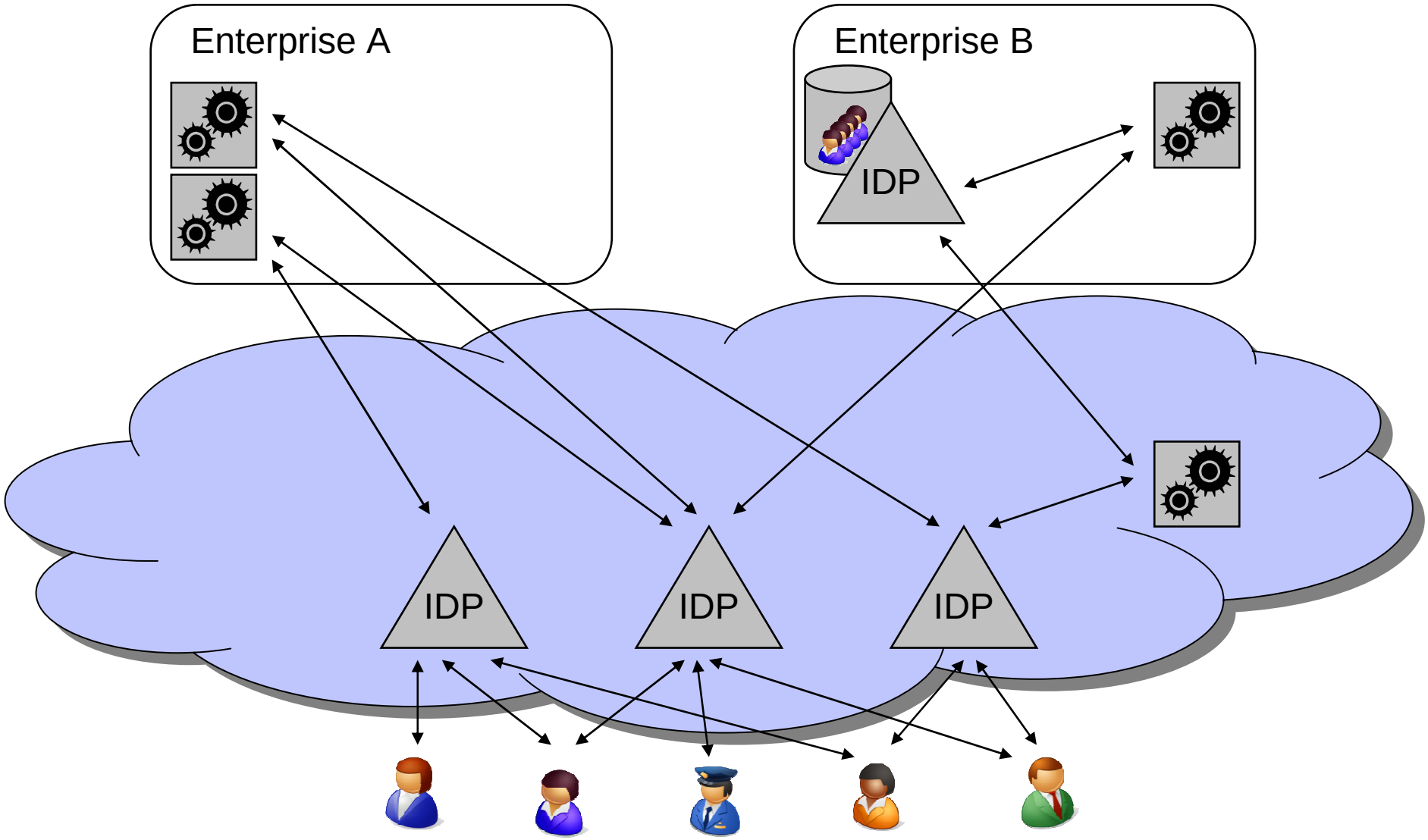




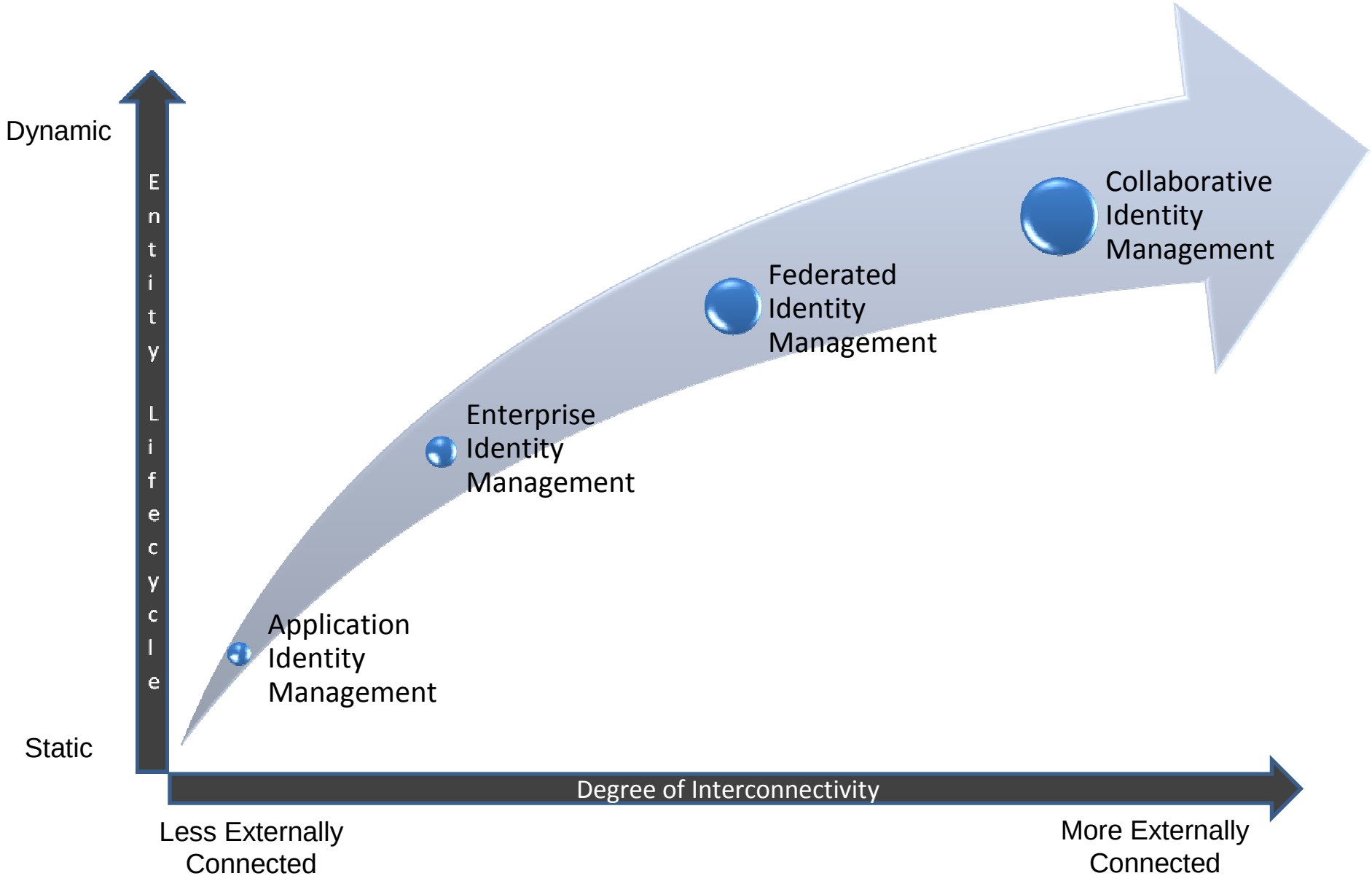
Federated identity management



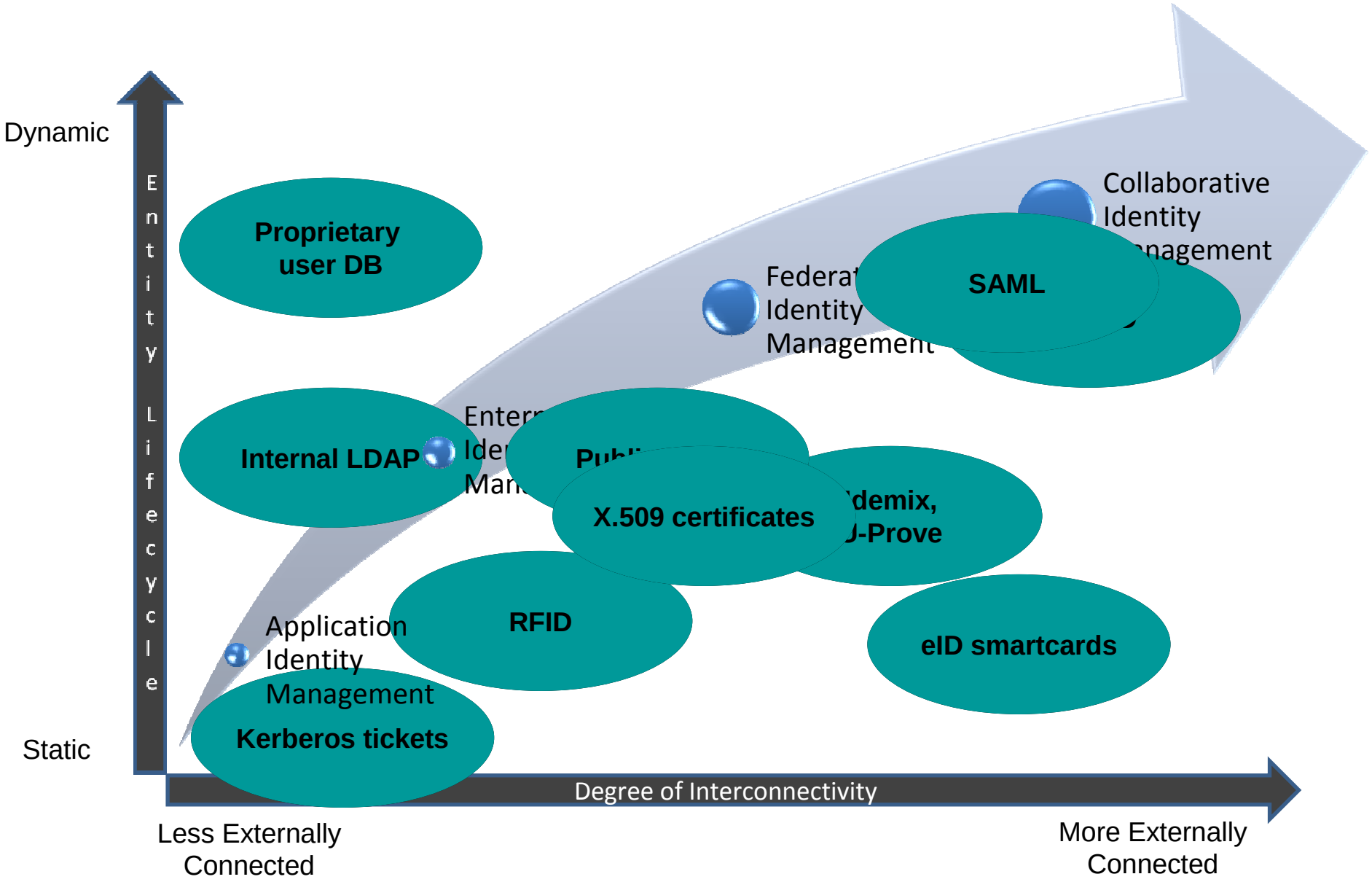
Collaborative identity management



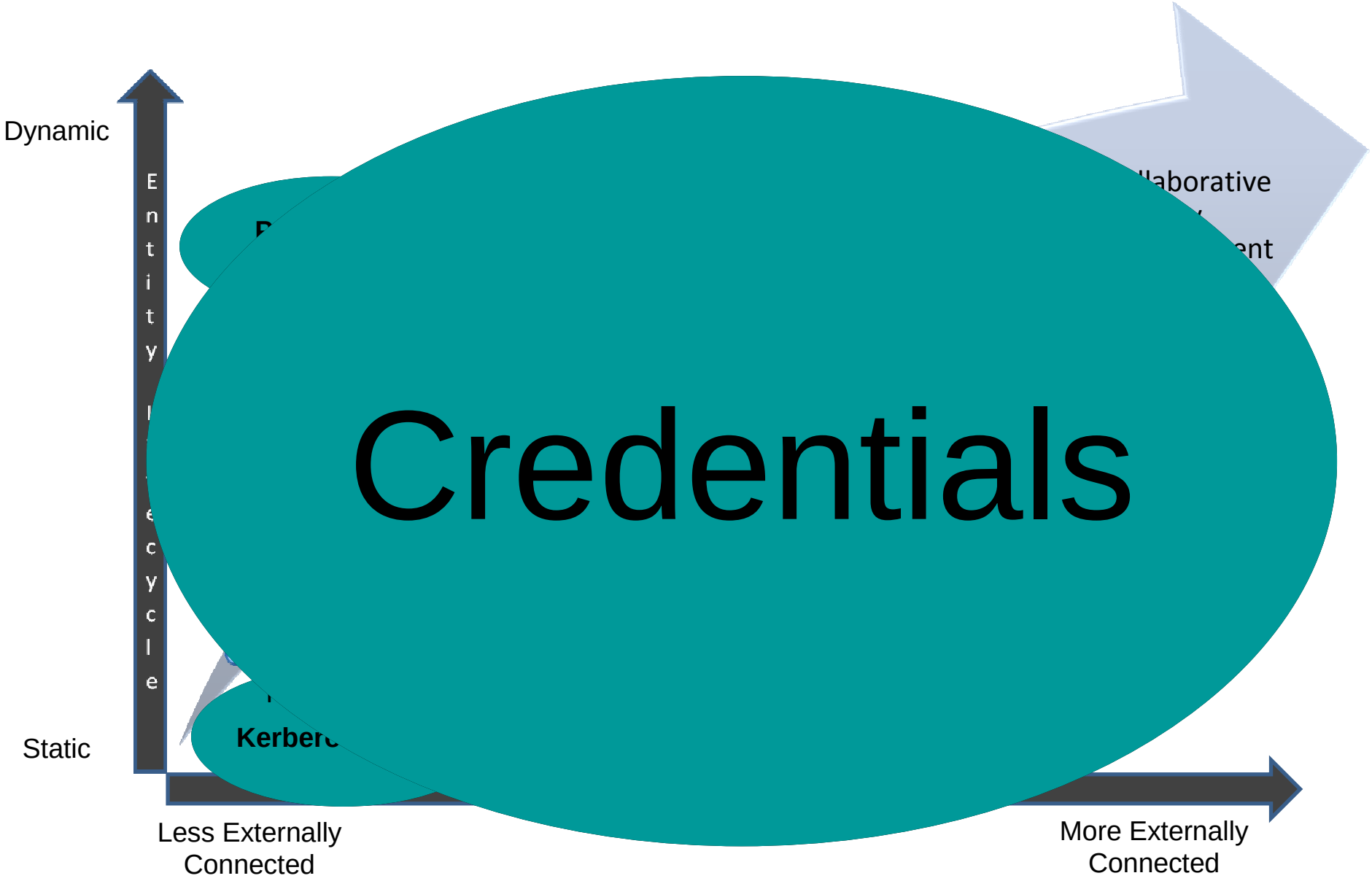
Trends in identity management



Trends in Identity Management



Trends in Identity Management



Credentials

- Credential: list of attribute values, certified by issuer
- Attributes describe user's identity (e.g., identity card), user's rights (e.g., credit card, concert ticket) or both (e.g., driver's license)
- Example technologies:

  X.509, SAML, CardSpace, OpenID, Kerberos, LDAP, Idemix, U-Prove,…
- Possible additional features:
  - attribute authentication
  - proof of ownership
  - (selectively) reveal attributes
  - prove condition on attributes
  - (selectively) reveal attributes to third parties
  - sign statements
  - limited spending

Language requirements

- Reference to individual credentials, (attribute-id, issuer) doesn't suffice
  - Credential types

    e.g. reveal name as on govt-issued passport, not ID card

    extensible OWL ontology of attributes and credential types
  - Credential mixing

    e.g. reveal number, expiration from **same** credit card
  - Cross-credential conditions

    e.g. passport.name = creditcard.name
- Distinguish between "reveal attribute" and "prove that condition holds"

  e.g. reveal birth date vs. age>18
- Provisional actions:

  Sign statements, reveal to 3rd party, limited spending

Example policy

own *p*::Passport **issued-by** USAgov

own *r* ::ResidencePermit **issued-by** ChicagoTownhall

own *c*::CreditCard **issued-by** Visa,Amex

reveal *c*.number , *c*.expirationDate **under** ‘purpose=payment’

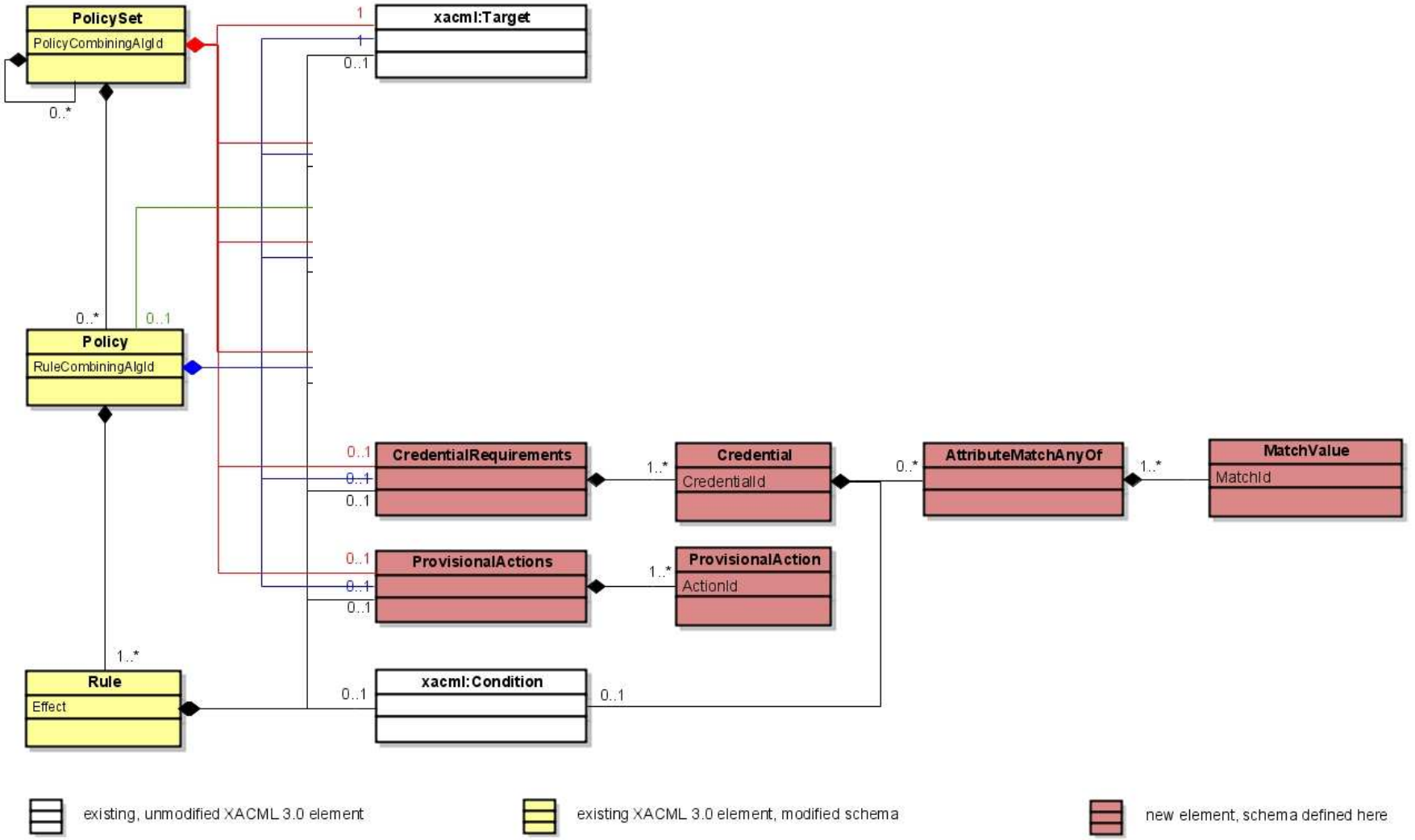
reveal *r*.address **to** ShippingCo **under** ‘purpose=shipping’

sign ‘I agree with the general terms and conditions.’

where *p*.dateOfBirth ≤ dateMinusYears(today(), 21) ^

c.expirationDate > today()

Embedding into XACML



Embedding into SAML

- New SAML statement types to carry
  - conditions on attributes using `<xacml:Condition>`
  - provisional actions
- Extend SAML assertion authentication to any type of proof token, e.g.
  - `<ds:Signature>`
  - LDAP server/password
  - Idemix proof
  - …

Summary

- Credential-based access control
  - attributes grouped in credentials
  - show multiple credentials simultaneously
  - technology independence
- Privacy enhancements
  - reveal attributes vs. prove condition
  - support anonymous credentials
- Embedded into XACML & SAML