Choosing the Best Identity Management Technology for your Business

Radovan Semančík

InfoSeCon 2006

nLight

Introduction

- **Complexity**

  Systems are networked and Internet-worked

  Virtualization, Outsourcing, Software as Service, ...

- **User Management**

  Did not change since 60s

  Manual, Slow, Unreliable

- **Need for a change: Identity Management**

  Better, faster and dependable User Management

  Distributable Authentication, Authorization, ...

Agenda

- **Enterprise Identity Management**

  Traditional **Enterprise** environment

- **User-Centric Identity Management**

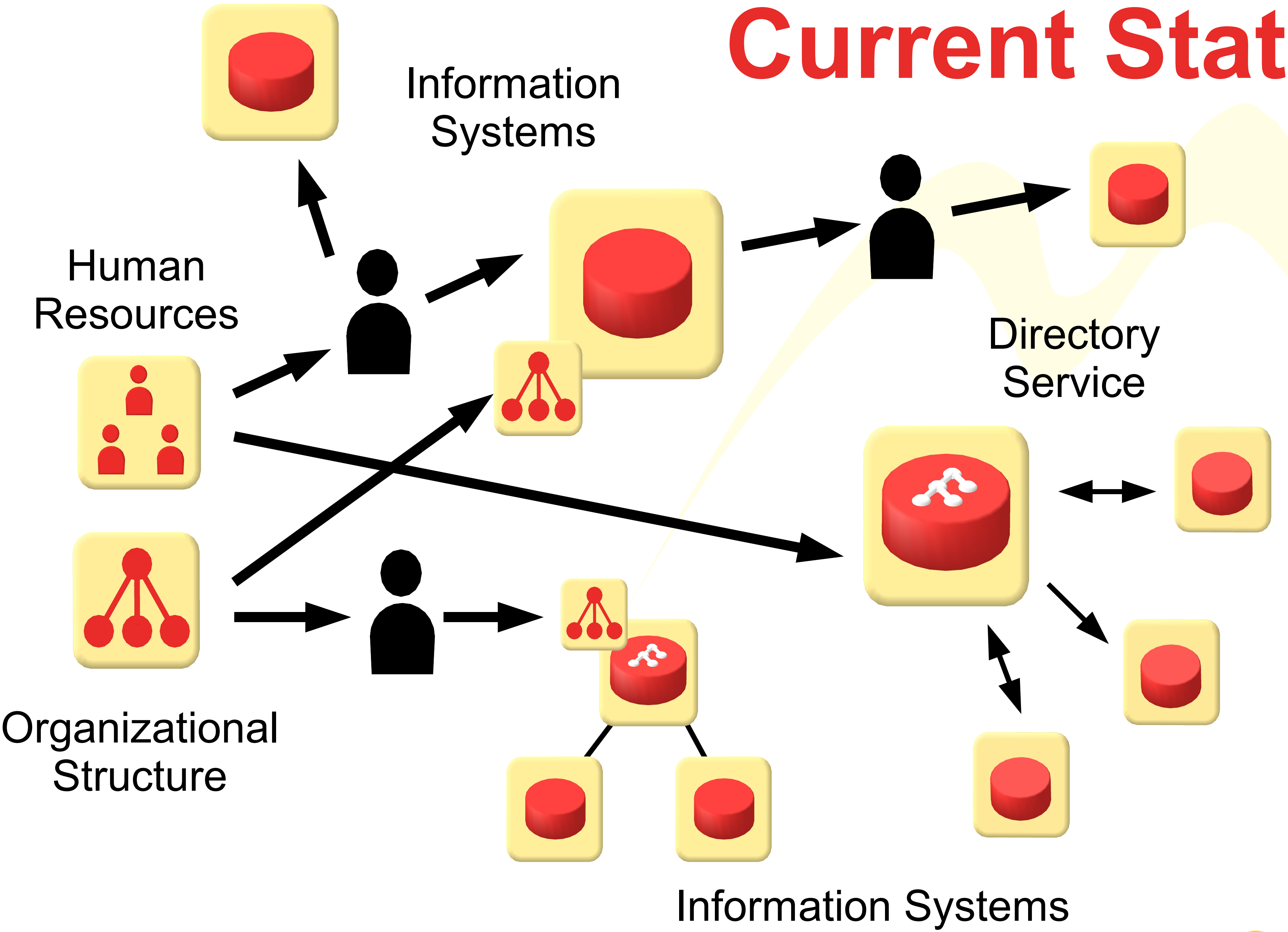
  Internet and distributed systems

- **Government Identity Management**

  Government information systems, eGovernment

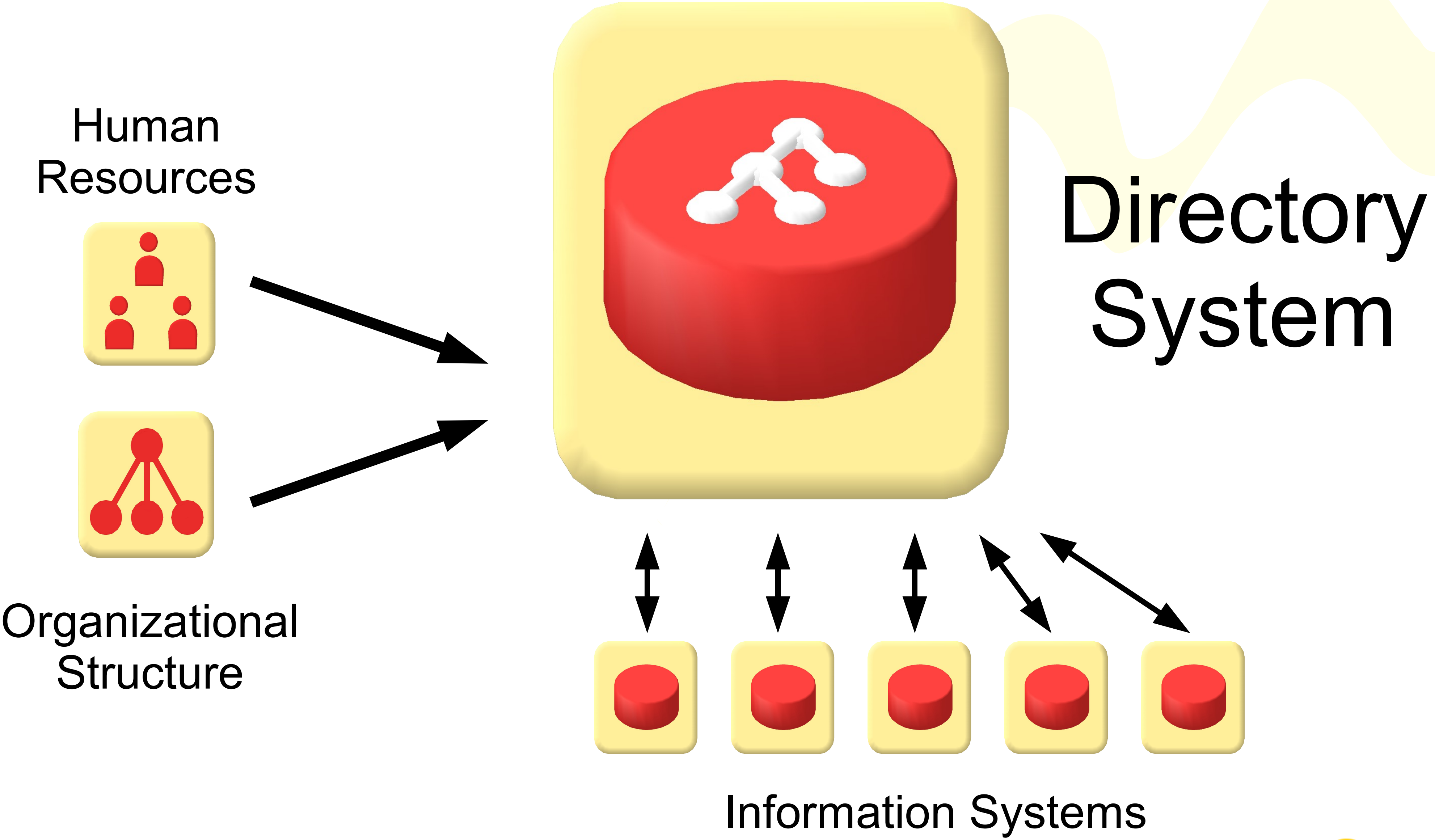
Enterprise Identity Management

Current State



nLight

Single Directory Paradigm



Human Resources

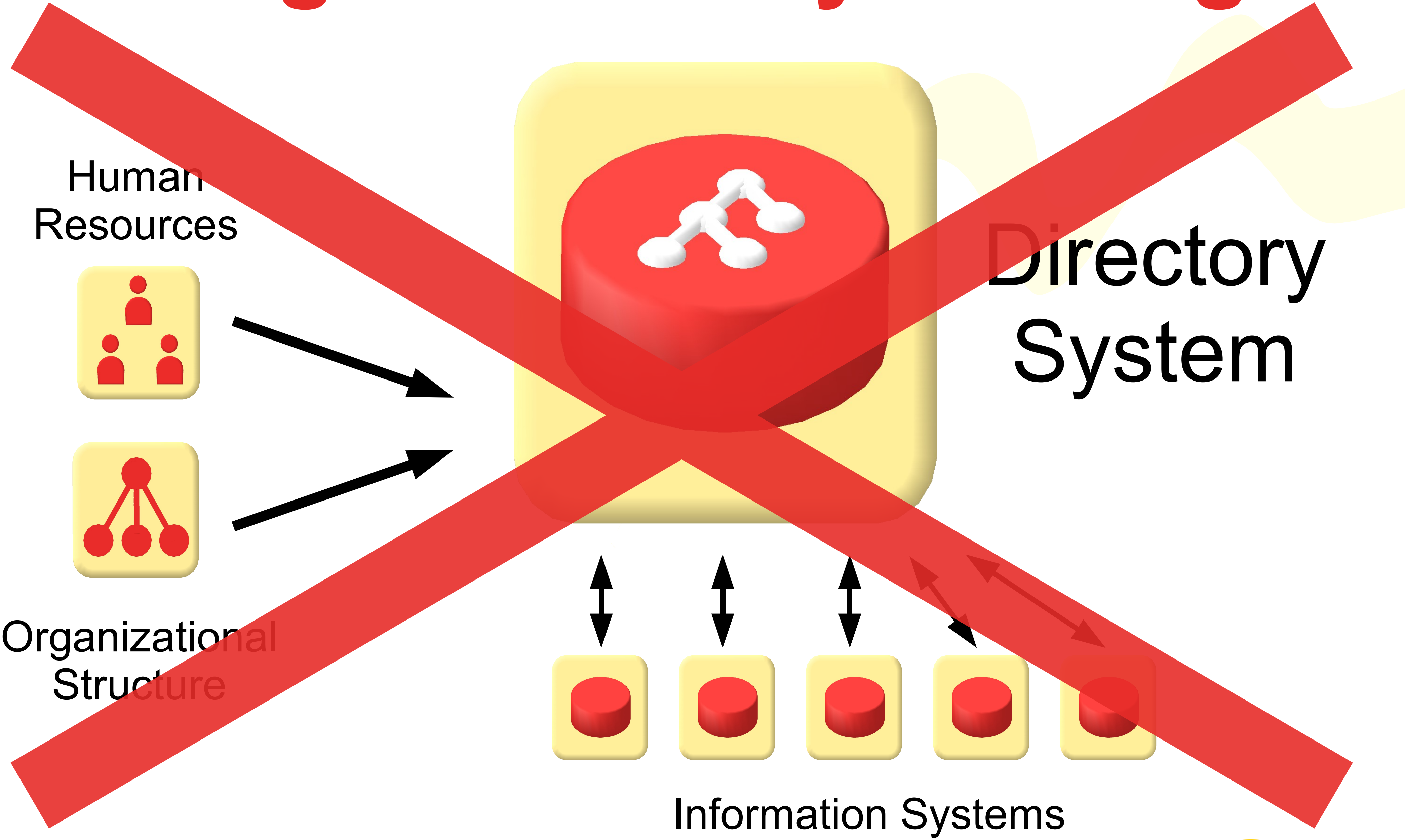
Organizational Structure

Directory System

Information Systems

nLight

Single Directory Paradigm



Enterprise IDM Challenges

- **Multiple Sources of User Data**

  Employee No., Tel. Number, E-Mail Address, ...

  Organizational Structure: Functional, Project, Effective

- **Stateful Services**

  Requirement to keep service state: Home Directrories, Mailboxes, historical records, ...

- **Inconsistent Policies**

  Different identifiers, Different permissions and roles, ...

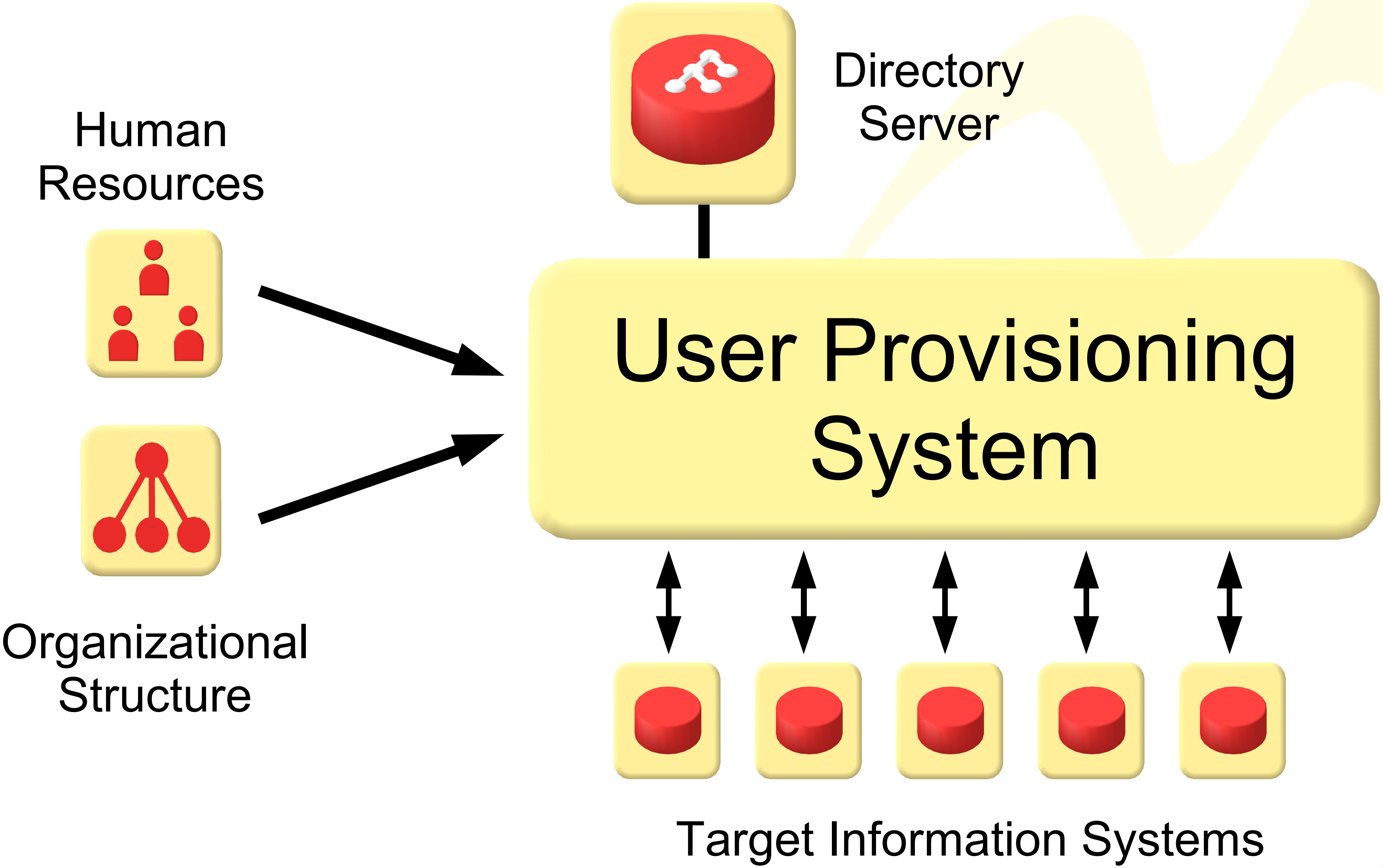
- **Re-provisiong na De-provisioning**

  Name changes (e.g. marriage)

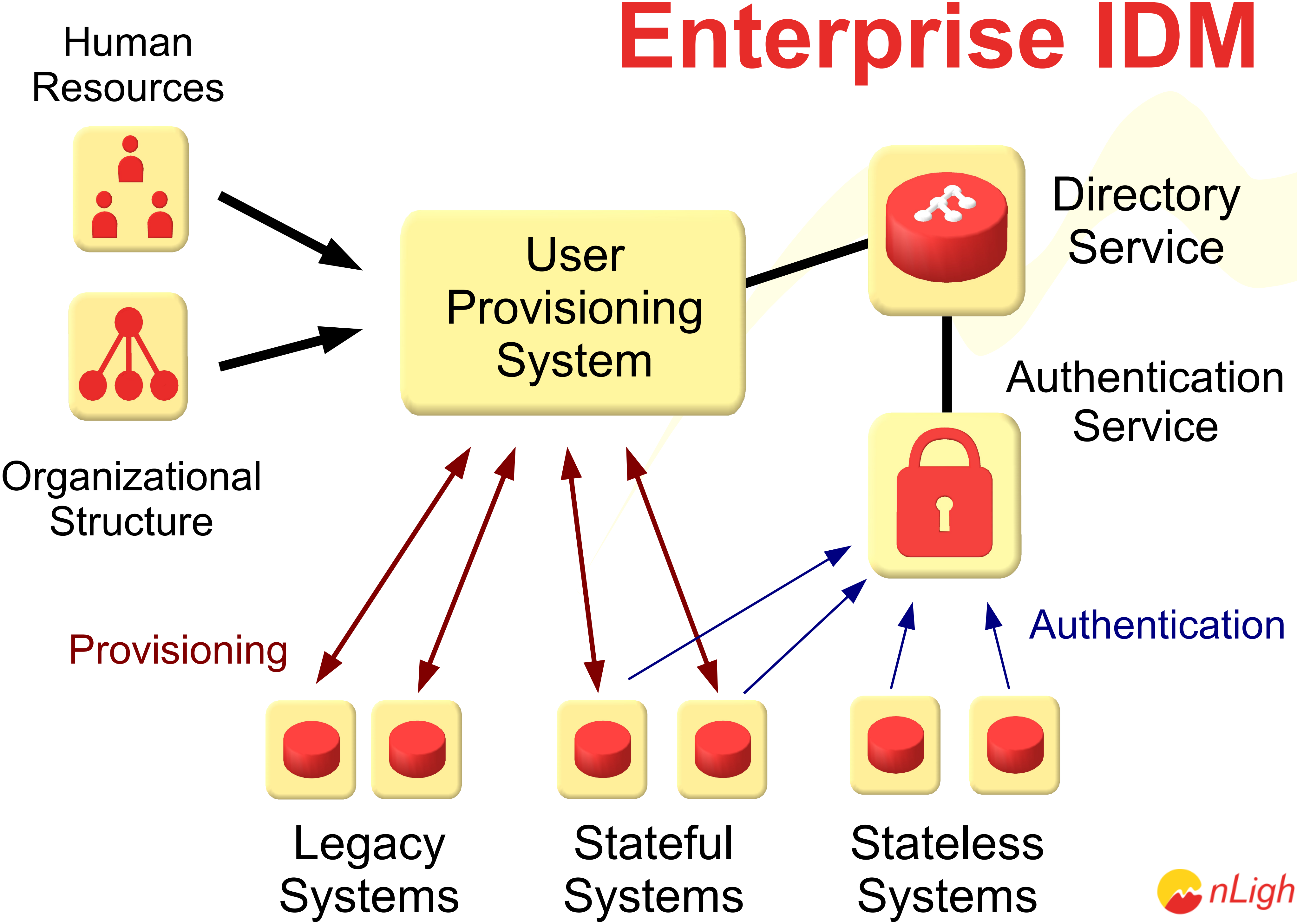
  Disposing of unused accounts

nLight

User Provisioning



Enterprise IDM



nLight

Enterprise IDM Solution

- **Provisioning System**

  Manages state of the information systems

- **Directory Services**

  Provide common repository of user information

- **Authentication Services**

  Maintain user session, provide Single Sign-On, ...

- **Future: Service Oriented Architecture**

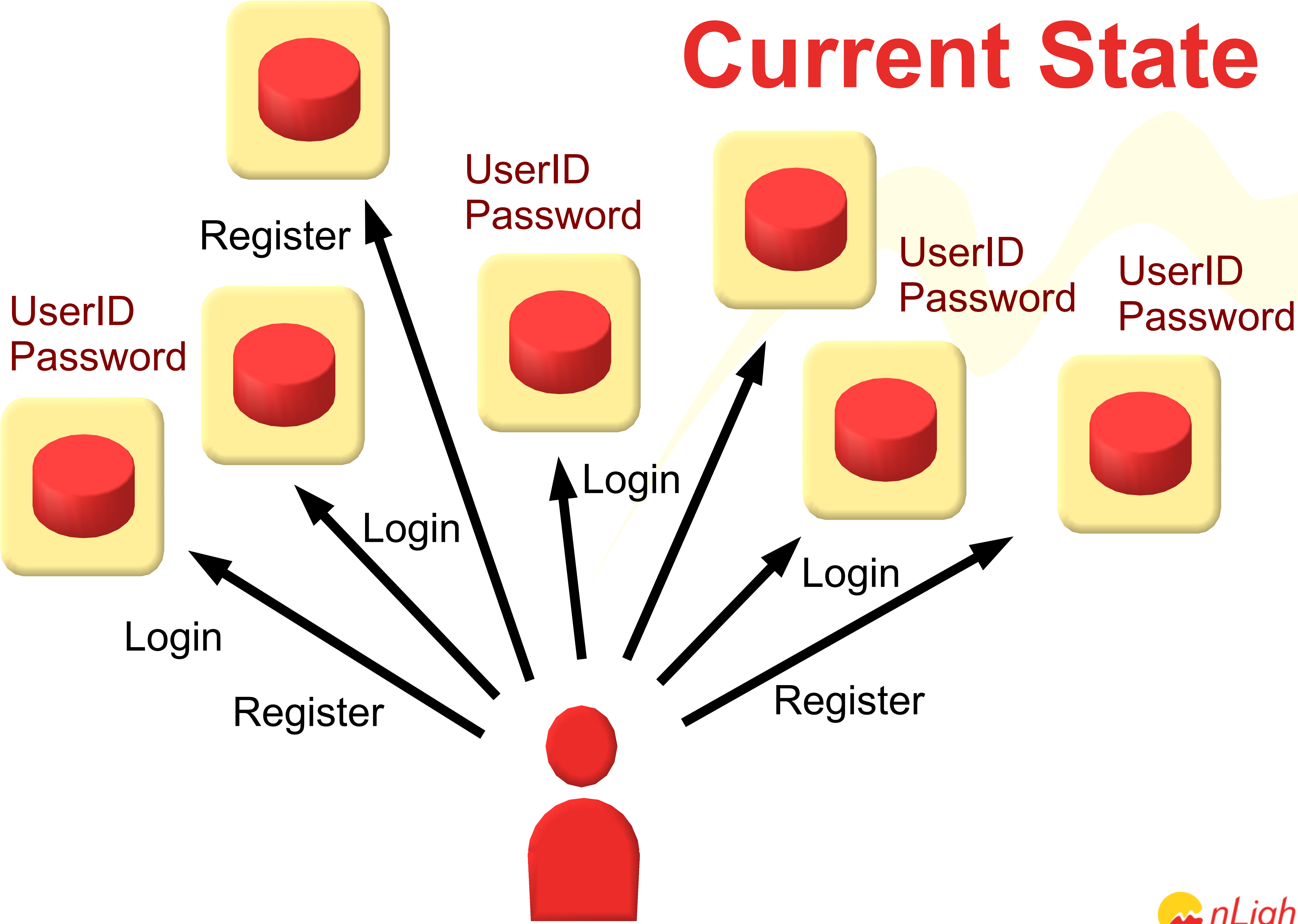
  Identity Services

User-Centric Identity Management

Identity Management for the Internet

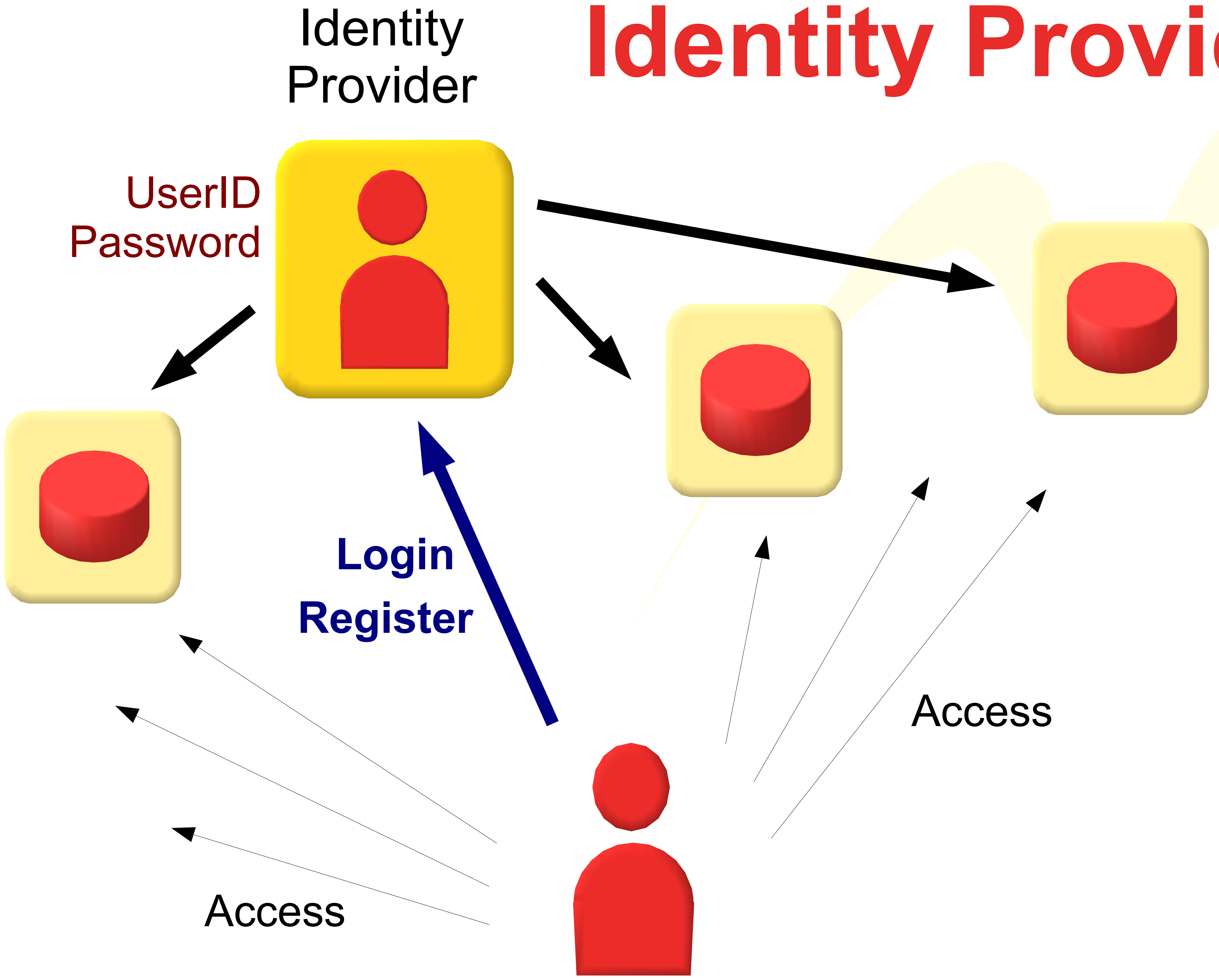
nLight

Current State



nLight

Identity Provider



User-Centric Identity

- **Simplifies Management of Personal Data**

  Keeping track of what data were submitted

- **Enabler for “Web 3.0” Applications**

  Distributed Social Networks

  Syndicating “Software as Service” Applications

- **Requires Trust**

  Current Identity Services require some level of trust to Identity Provider or other network components.

nLight

Government Identity Management

nLight

Government Digital Identity

- **X.509: Traditional Method**

  Expensive, cumbersome and inflexible

  Fixed identifier in certificate allows tracing user

  Government certificates usable only for G2C

  Insecure on common workstations

- **Alternative?**

  Not really

- **What to do?**

  Use Enterprise methods to clean up identity stores

  Invest in research

Common Identity Problems

- **Global Identifiers**
  - SSN, E-Mail Address, URLs, ...
  - May cause loss of privacy
- **Insecure Workstations**
  - Malware can compromise most PCs
  - If workstation cannot be trusted, nothing can be secure.
- **Honeypot Effect**
  - Centralizing of personal data attracts thieves.
  - Both server-side and client-side

nLight

Conclusion

- **Enterprise Identity Management**
  - Effective, real value
  - Will be needed for next generation architectures
- **User-Centric Identity**
  - Under heavy development, may be usable in near future
  - Will enable “Web 3.0” applications
- **Government Identity**
  - X.509 is not really effective
  - Further research is needed

nLight

Thank You

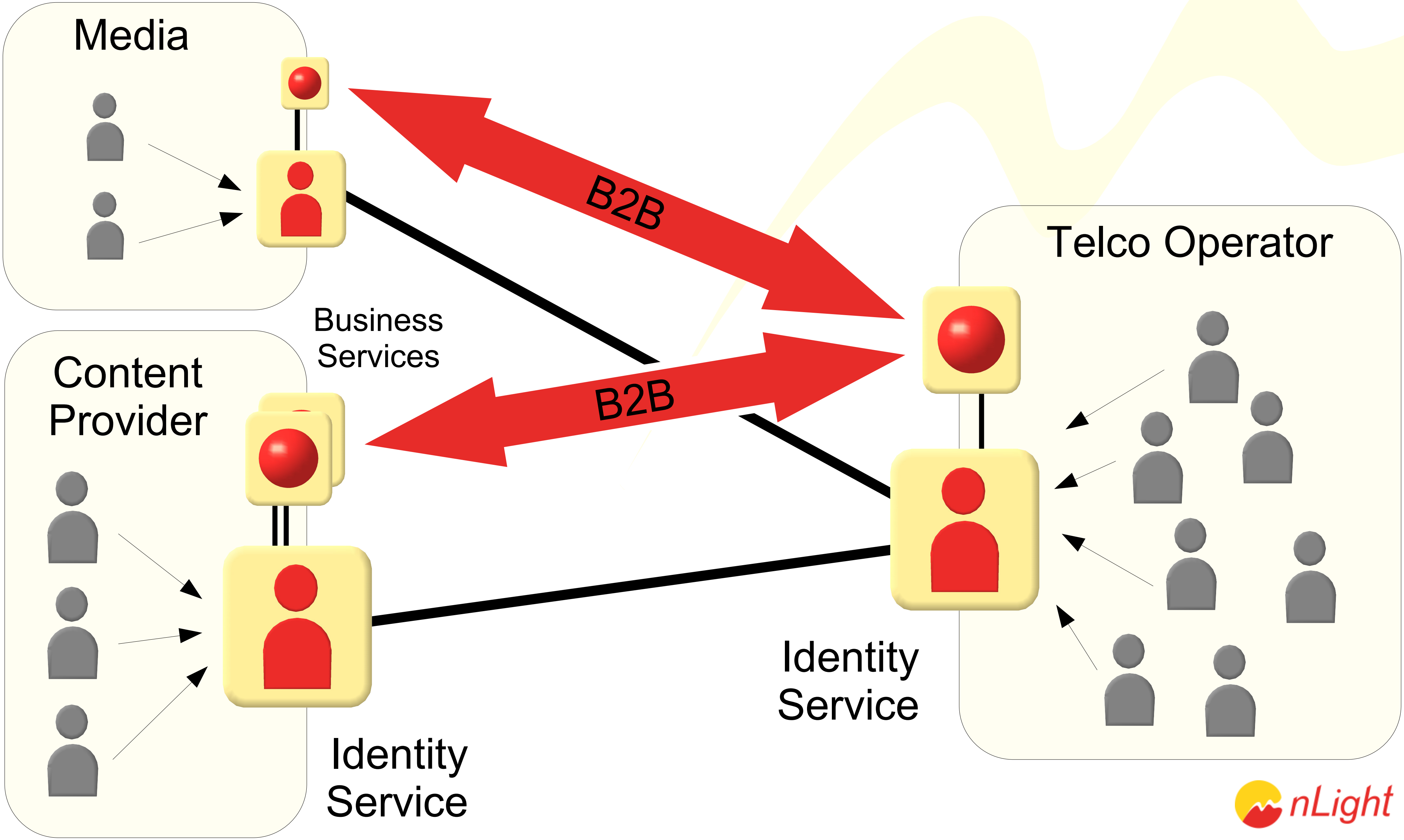
Radovan Semančík
nLight, s.r.o.

semancik@nlight.sk
www.nlight.sk

Extra Slides

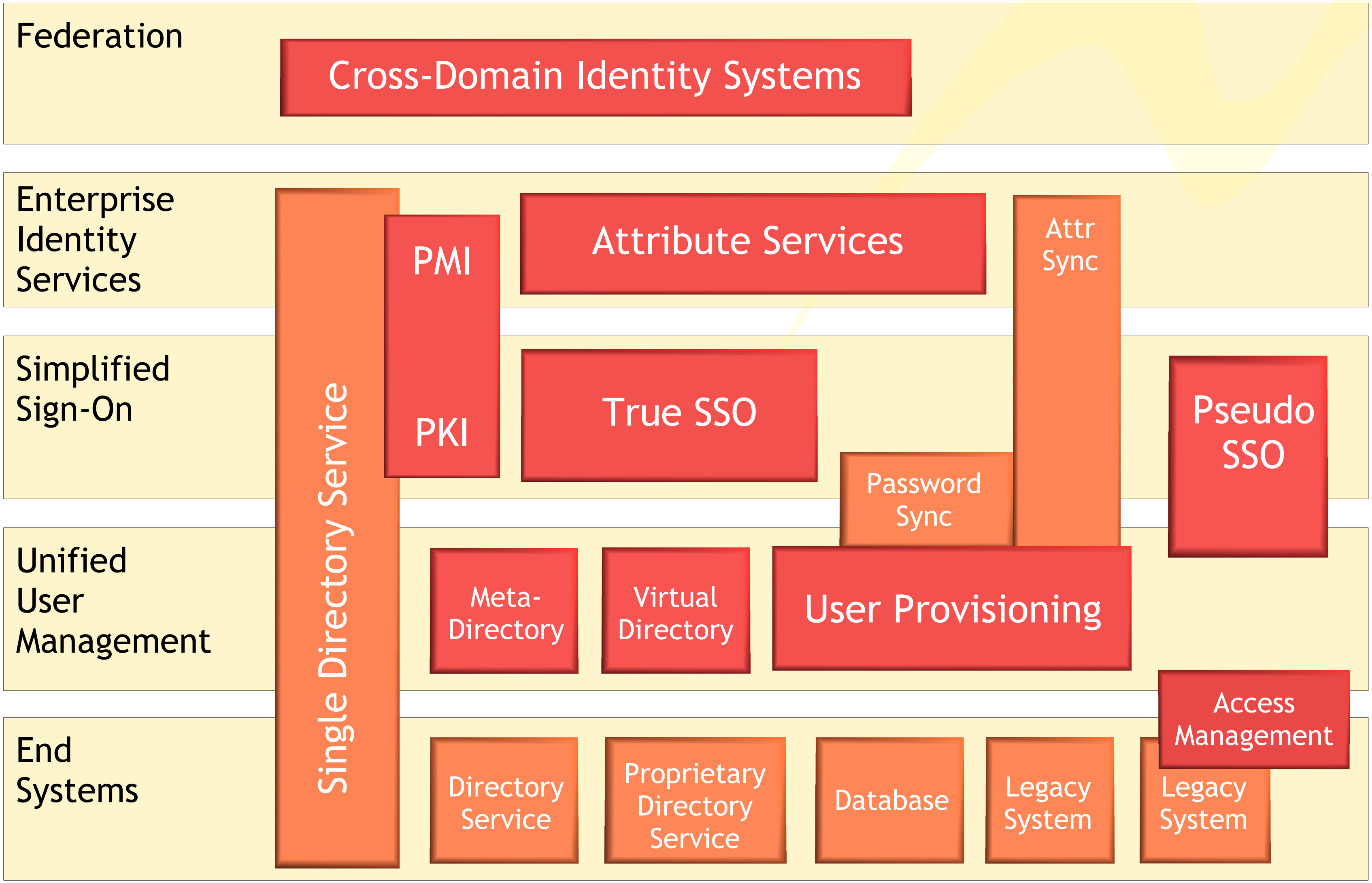
nLight

Cross-Domain Identity



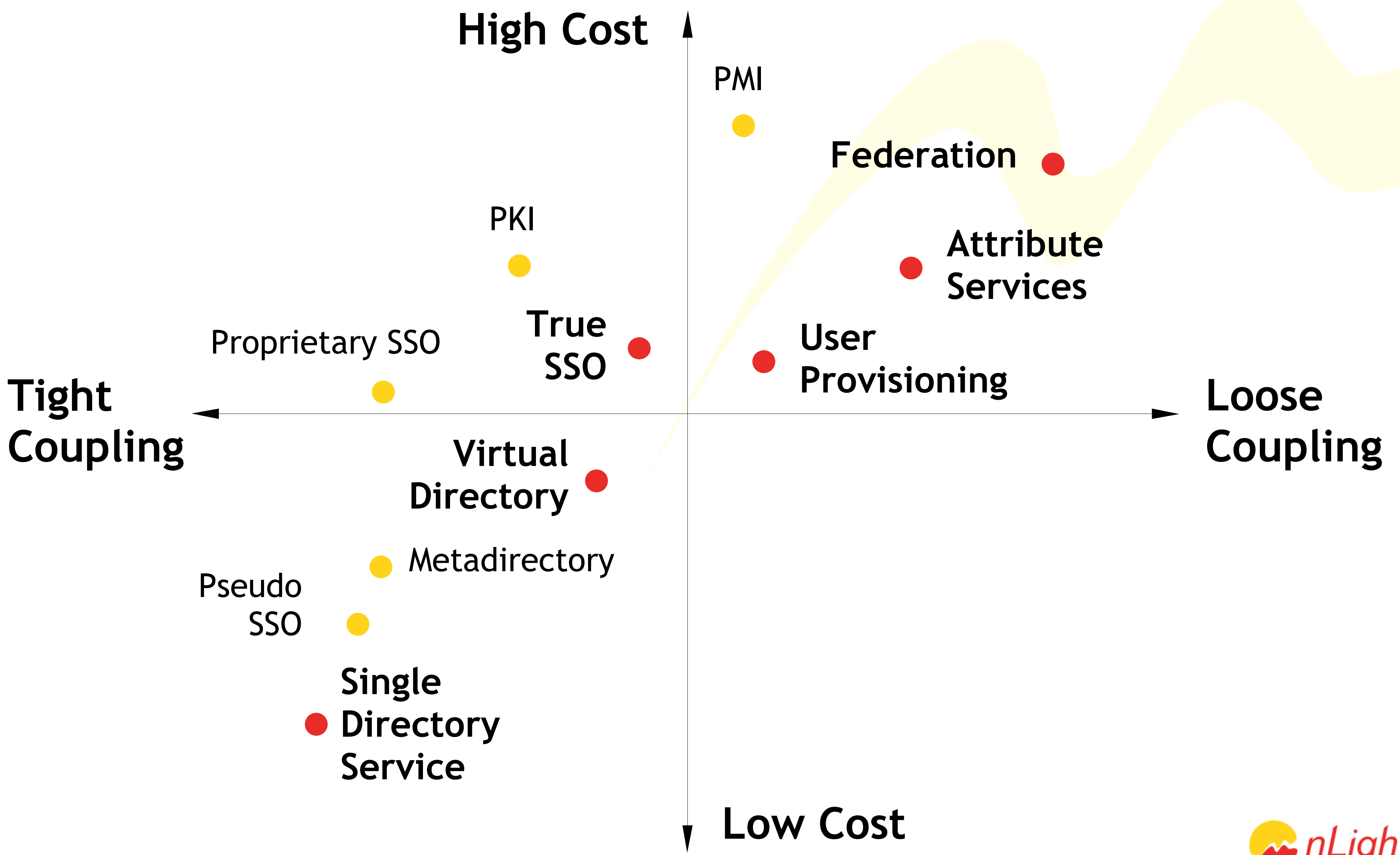
nLight

Identity Management Technologies



nLight

IDM Technolgies Compared


High Cost
PMI
Federation
PKI
Attribute Services
True SSO
Proprietary SSO
User Provisioning
Tight Coupling
Loose Coupling
Virtual Directory
Metadirectory
Pseudo SSO
Single Directory Service
Low Cost