Digital Identity and PKI What's the Next Step?

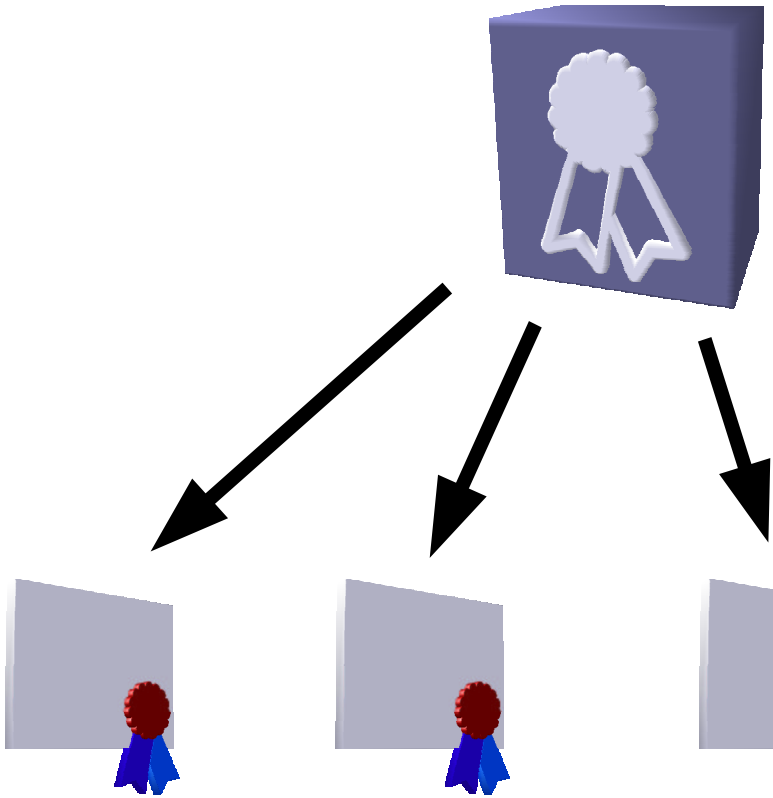
Radovan Semančík

BGS
Business Global Systems

Introduction

- **Public Key Infrastructure**
  - Infrastructure built on public-key cryptography
  - Especially X.509-based infrastructures
  - “ Digital certificates”, “Electronic signatures”, CAs
- **Digital Identity, Network Identity**
  - XML-based, Internet “security” infrastructure
  - Mostly LDAP-based “Unified User Management”
- **Simplified Sign-On** (Single Sign-On)
  - Authentication infrastructure
  - Kerberos, Passport, Liberty (Phase I), ...

Public Key Infrastructure



Certificate Authority

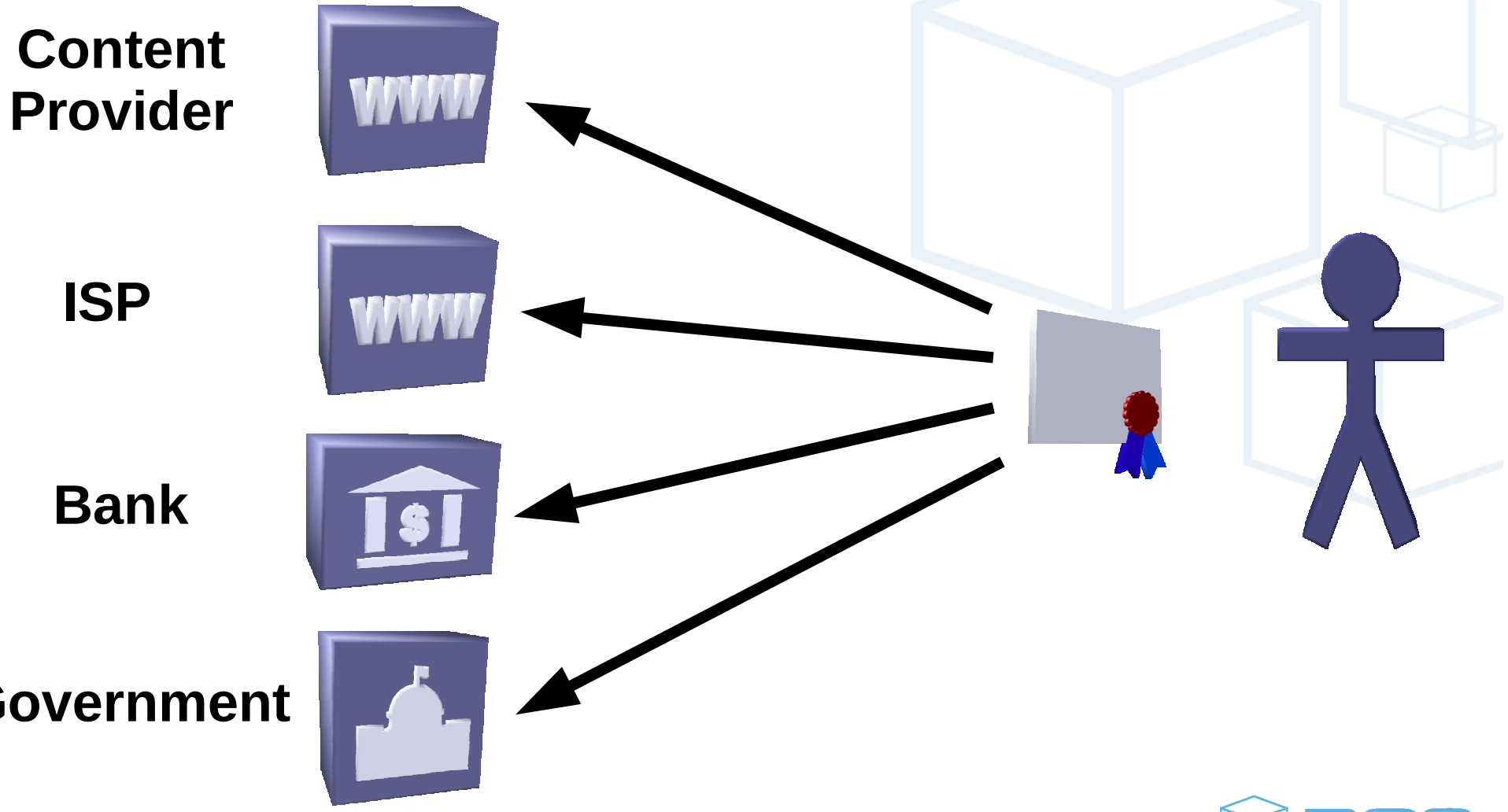
Public Key Certificates

BGS Business Global Systems

Public Key Certificate

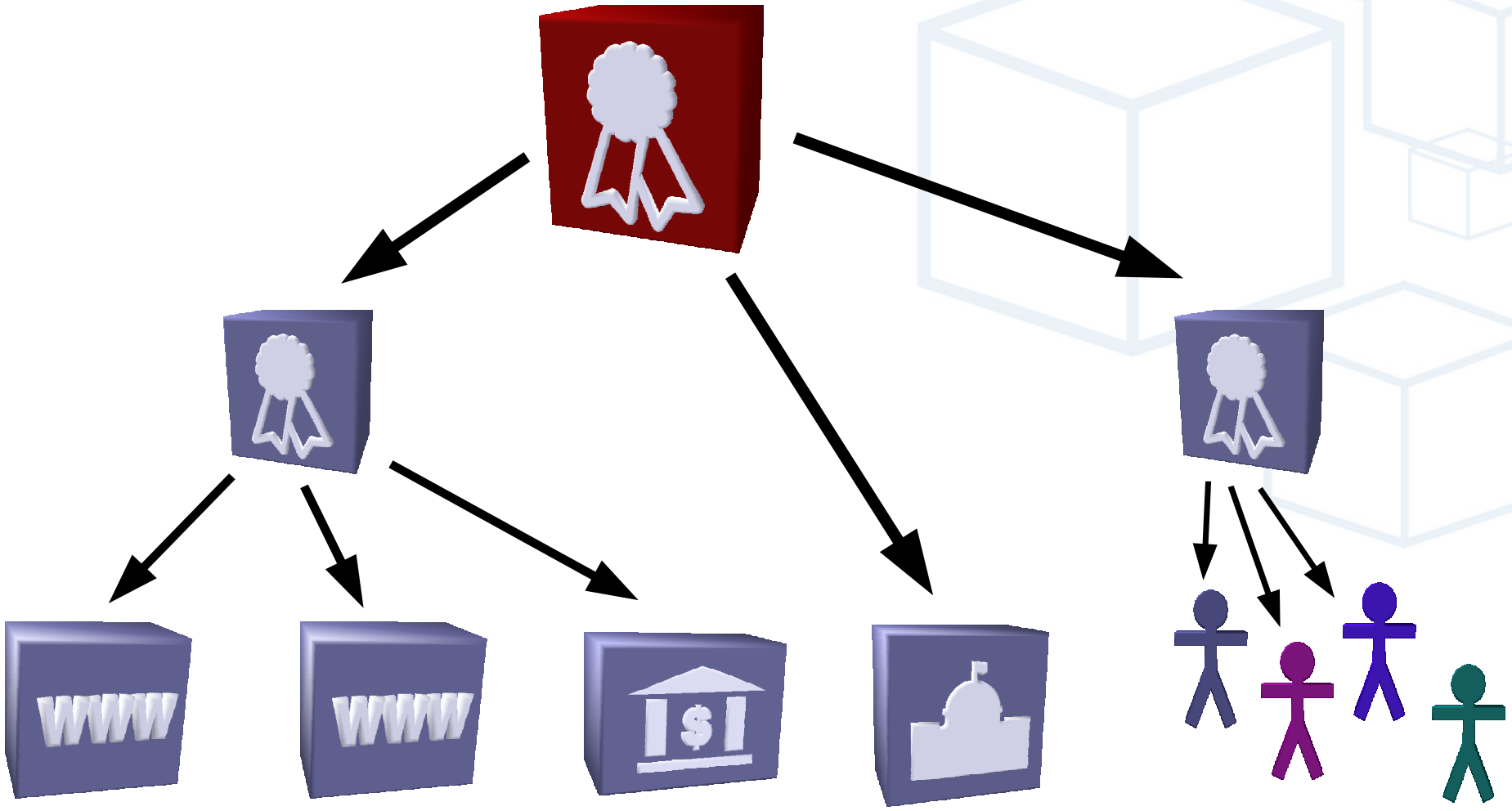
BGS Business Global Systems

How to Use Certificates (theory)



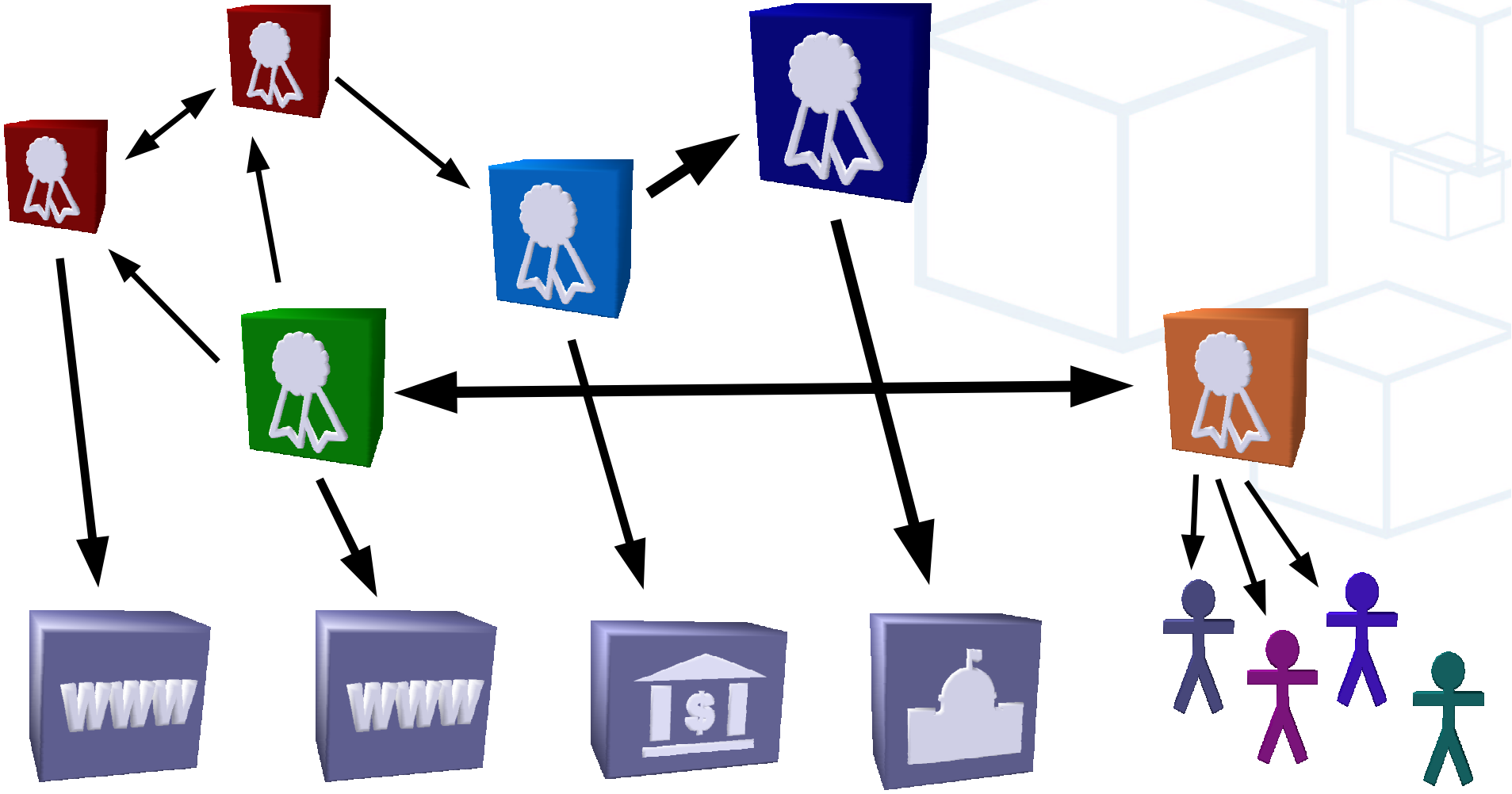
BGS
Business Global Systems

Single Root Authority



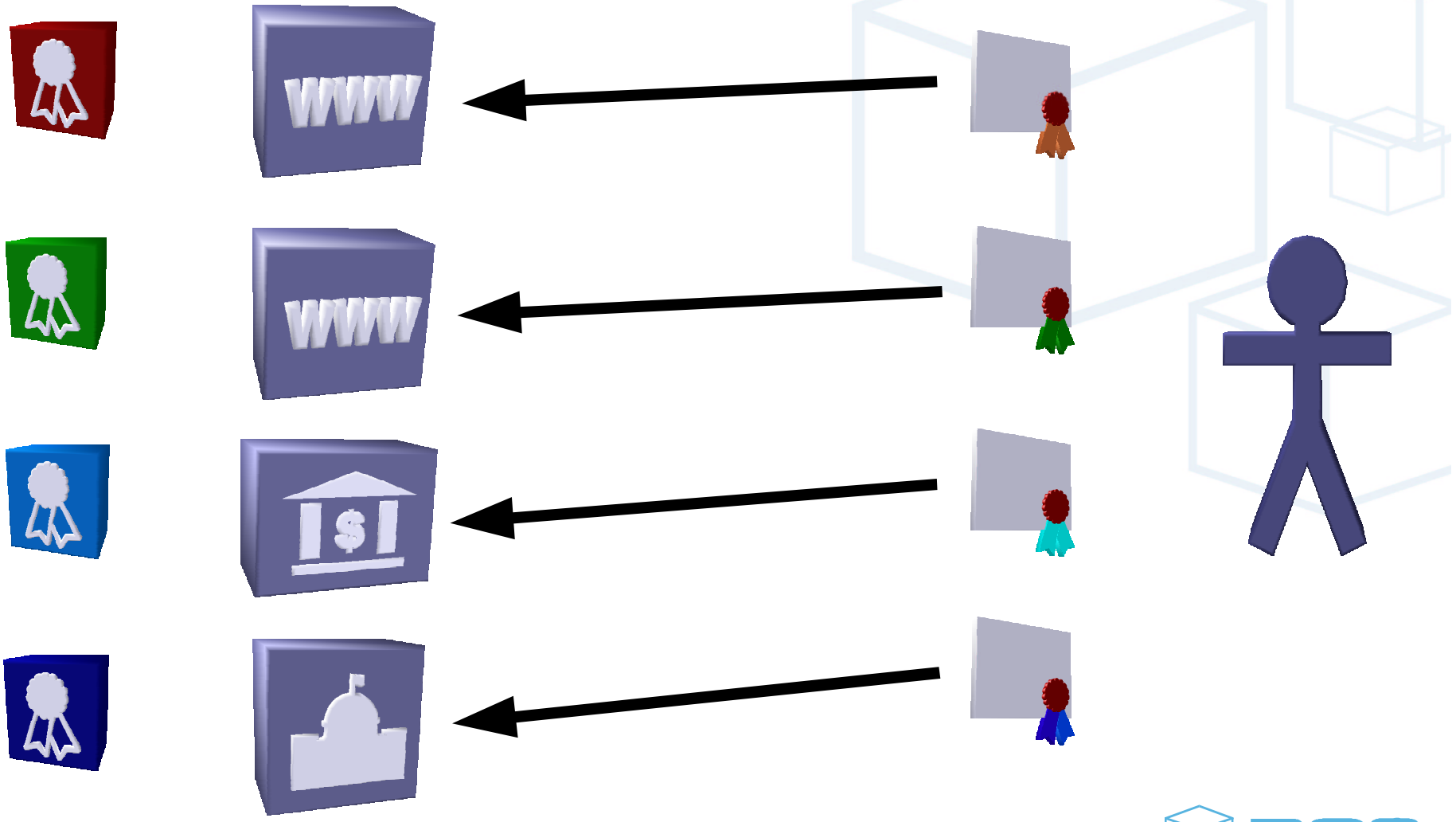
BGS
Business Global Systems

Real Situation



BGS
Business Global Systems

How to Use Certificates (practice)



BGS
Business Global Systems

Privacy & Others ...

Problems:

- Privacy
- Interoperability
- Access Control
- Privileges, Roles

- Low Flexibility
- High Cost

BGS Business Global Systems

What Should We Do?

(Identity Crisis)

BGS
Business Global Systems

Identity

Identity (n): collective aspect of the set of characteristics by which a thing is recognizable or known

WordNet

Language
Locality

Financial records
Helth records

SE35758423

rsemancik

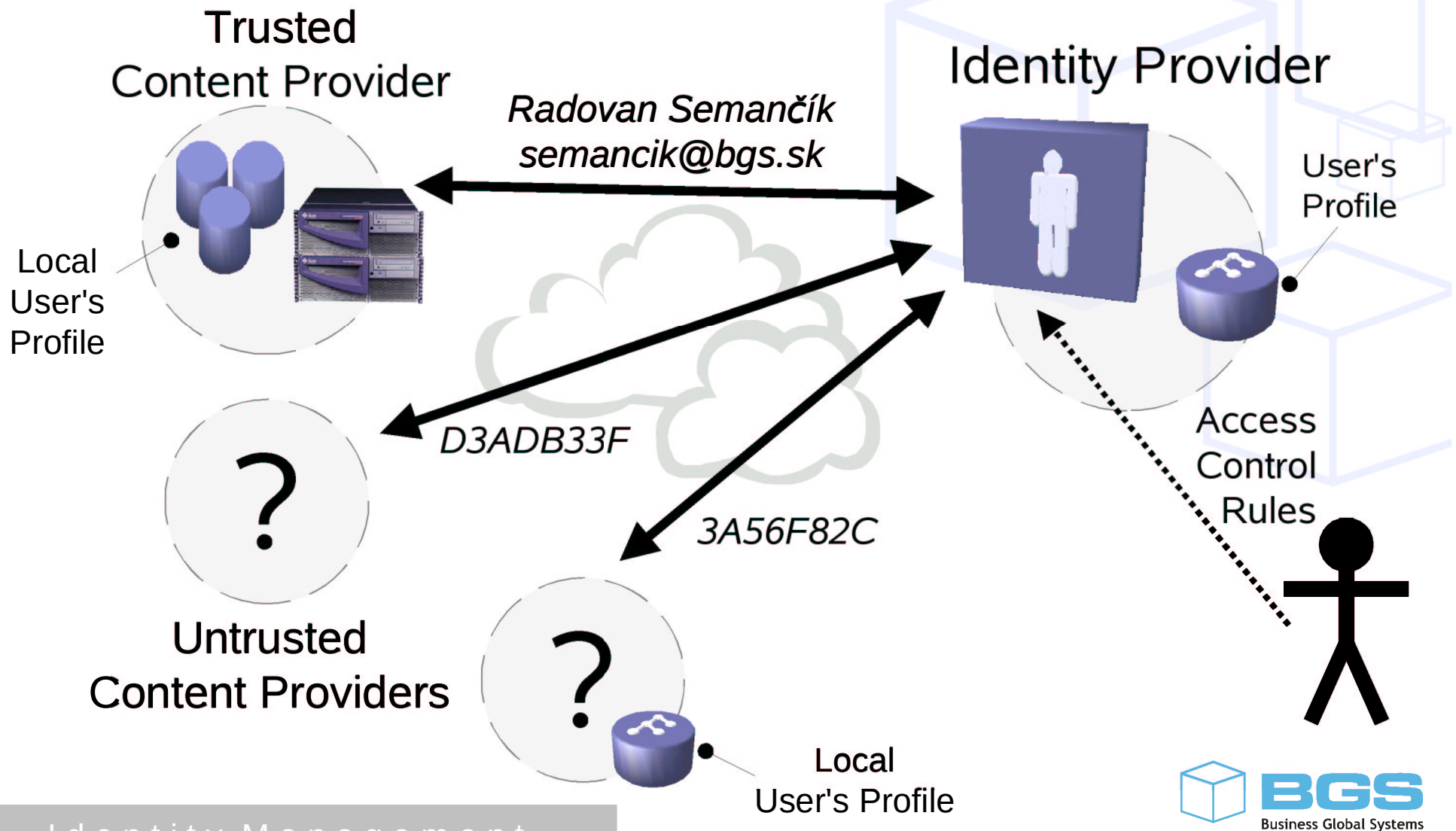
Shopping preferences
Travel preferences

Title, Role
Org. membership

Radovan Semančík

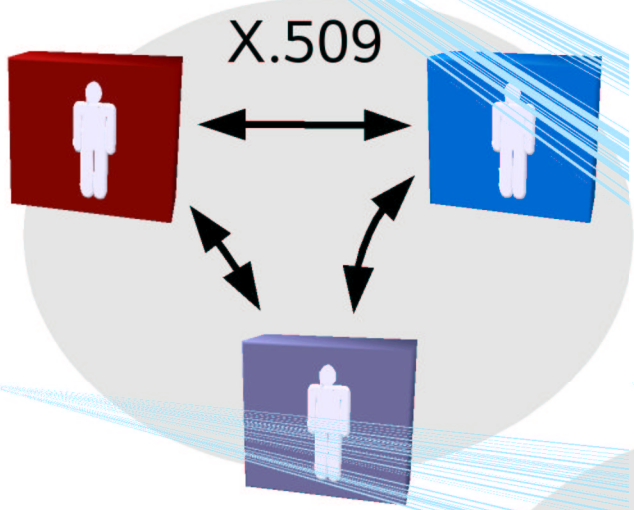
BGS
Business Global Systems

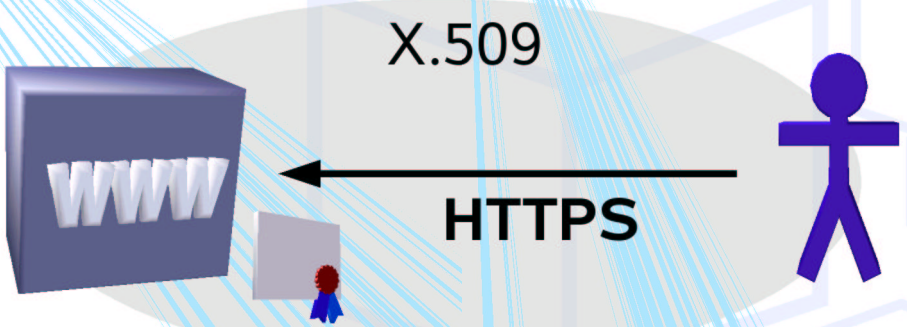
Identity Management

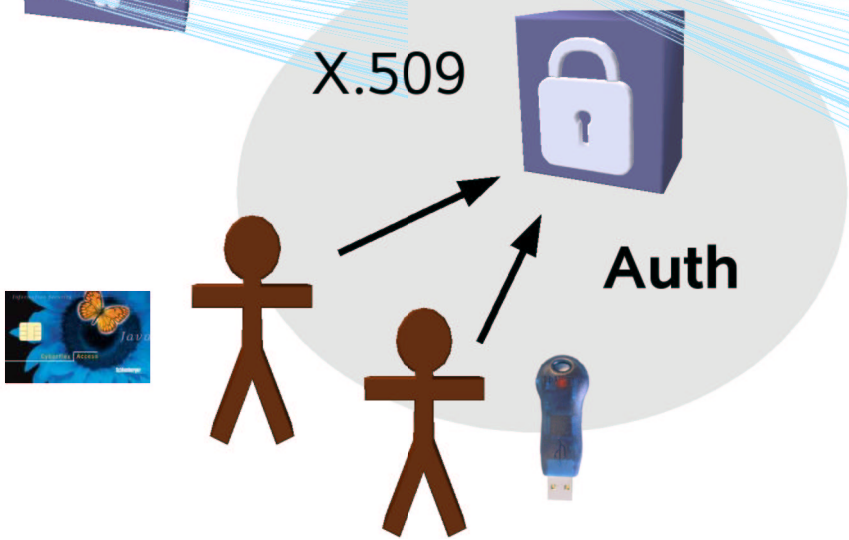


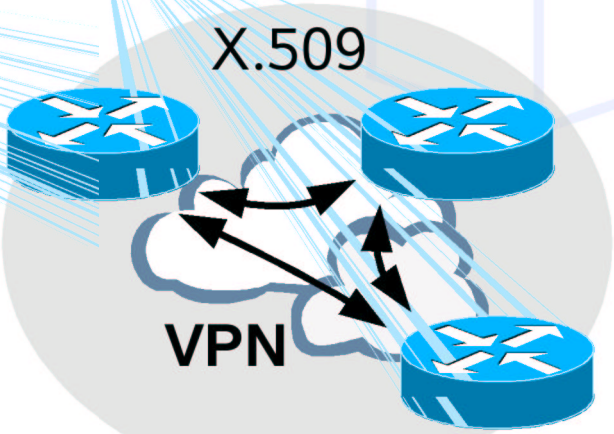
BGS
Business Global Systems

X.509 PKI is not Completely Wrong



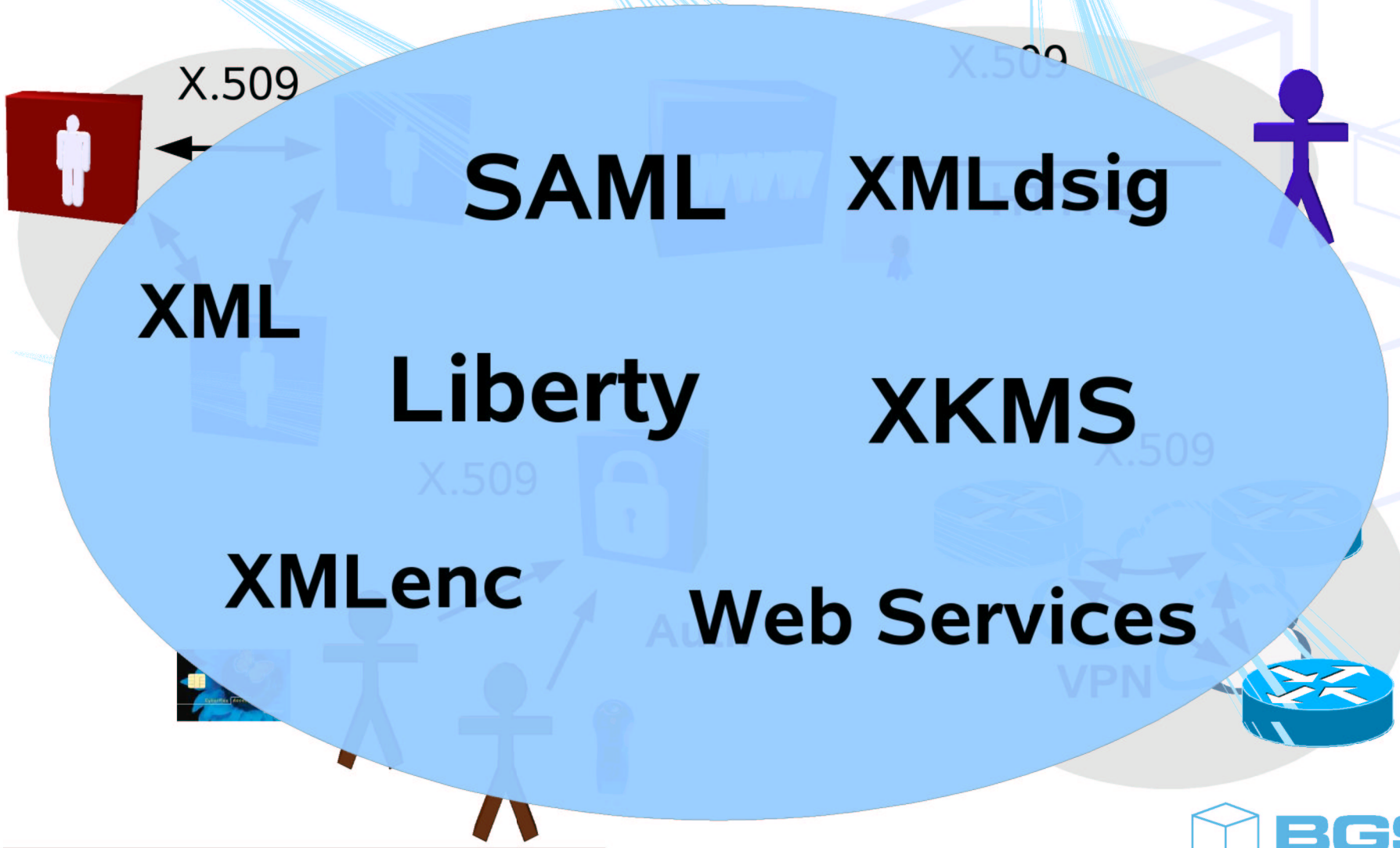






BGS
Business Global Systems

XML-based “PKI”



BGS
Business Global Systems

What To Do

1. **Rethink, Reinvent and Redesign PKI**
   - Focus on XML, Web Services, Standards
2. **Implement Identity Management**
   - Directories, SAML, Liberty, ...
3. **Take Advantage of New Infrastructure**
   - New Services, New possibilities

Questions?

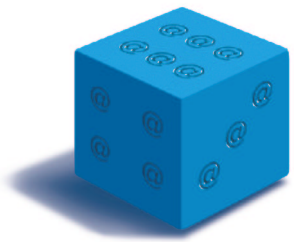
BGS
Business Global Systems

Thank you ...

Ing. Radovan Semančík

Business Global Systems, a.s.
Pluhová 2
83248 Bratislava

semancik@bgs.sk



BGS
Business Global Systems