

# PKI or not PKI? That's the question ...

Radovan Semančík



# Čo je to vlastne PKI?

a) Buzzword

a) Viac o buzzwordoch prednáška o 14:00

b)

b) Elektronický podpis a spol.

a) “To akože si naskenujem podpis a pripojím k mailu ...”

b)

c) Public Key Infrastructure

a) Asymetrická kryptografia, public/private key, bla bla bla

# Ako to bolo na začiatku?

**Alice**



telnet



**Bob**



Login: foo  
Password: bar



**Eve**

Eavesdropper

# Pokus ...

Alice

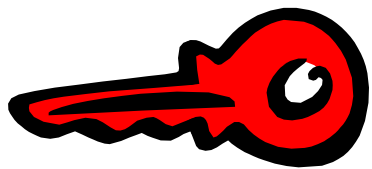


telnet

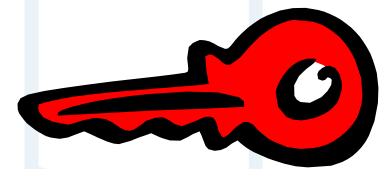


3DES

Bob



a#4bF3^hjdk&#WE0sdf  
jk234890723JH(\*#@#&\*i

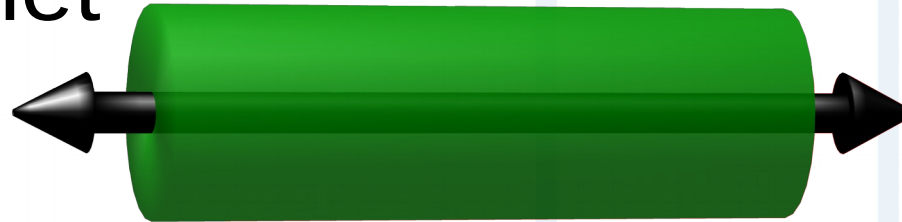


# Druhý pokus ...

Alice

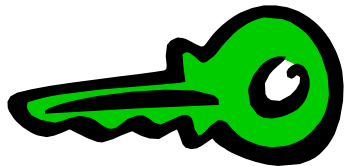


telnet

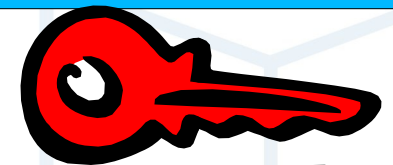


RSA

Bob



a#4bF3^hjdks&#WE0sdf  
jk234890723JH(\*#@#&\*i



# Pozor na Malloryho!

Alice

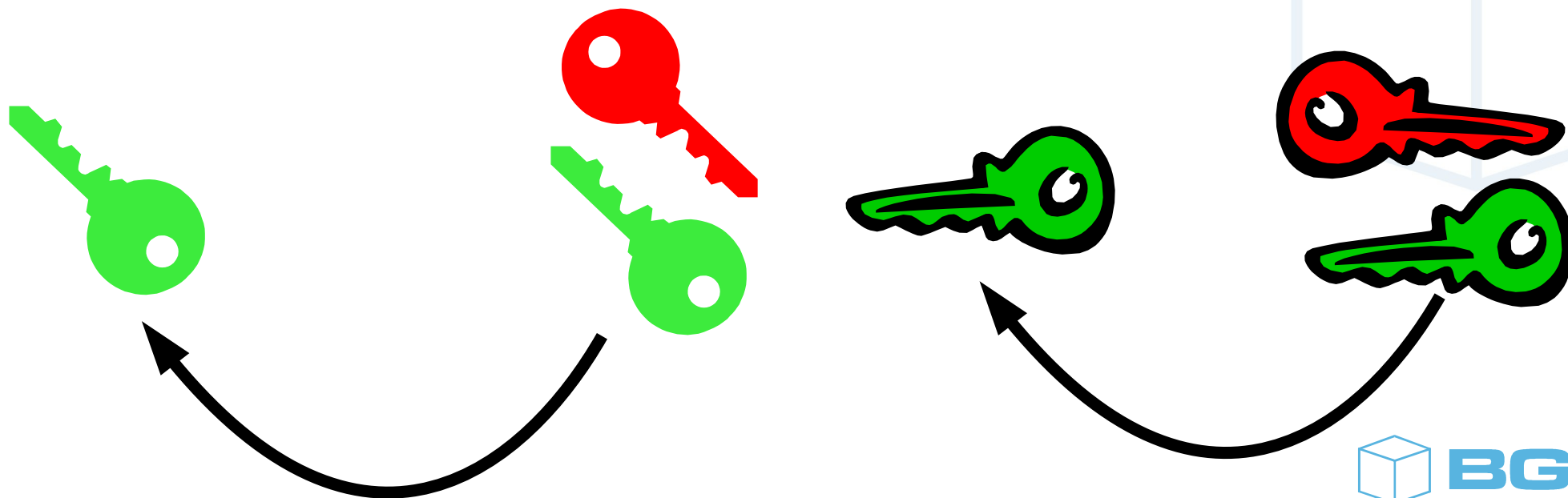


Mallory

Man in the Middle



Bob



# Public Key Certificate

Alice

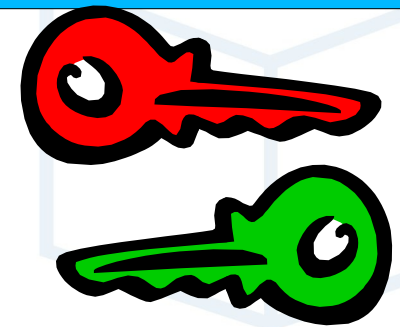
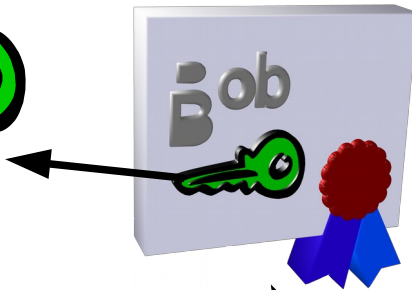


telnet



RSA

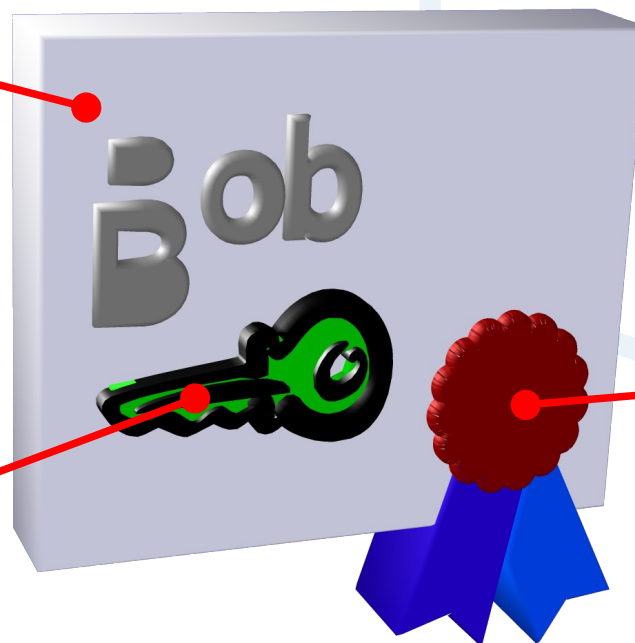
Bob



# Public Key Certificate

Meno

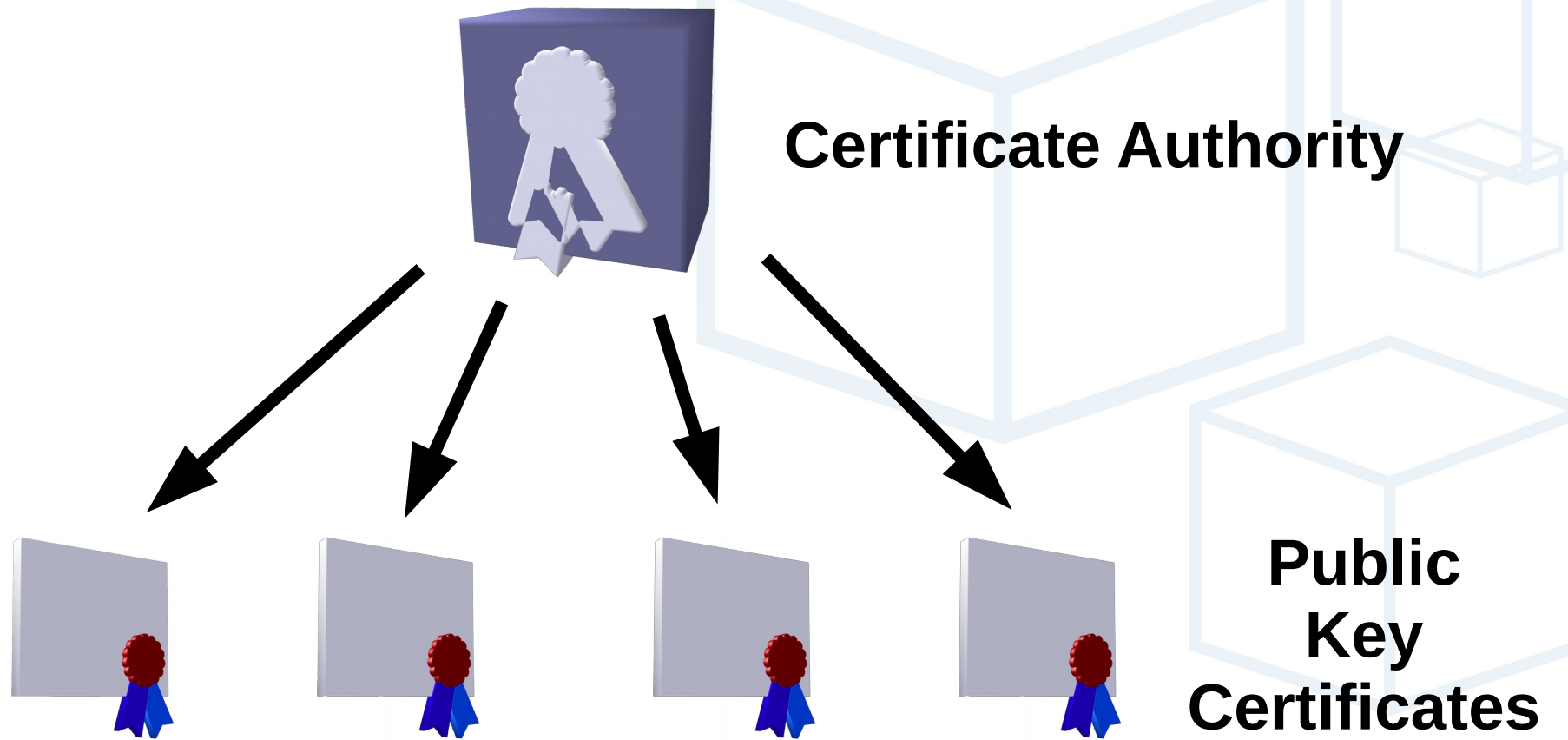
Verejný  
kľúč



Podpis  
dôveryhodnej  
tretej  
strany



# Certifikačná Autorita



# X.509

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 1 (0x1)

Signature Algorithm: md5WithRSAEncryption

**Issuer: C=sk, L=Horna Dolna, O=Druha Certifikacka, s.r.o., CN=CA**

Validity

Not Before: Mar 28 08:45:40 2003 GMT

Not After : Apr 27 08:45:40 2003 GMT

**Subject: C=sk, L=Dolny Vyplach, O=JozoFero, s.r.o., CN=www.jozoafero.sk**

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Modulus (1024 bit):

00:ba:74:1b:4f:c6:e2:2e:92:ce:b1:2c:3b:51:ca:

...

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Subject Key Identifier:

66:32:4C:2C:D7:83:1E:EC:6C:0D:4D:DB:AA:3C:BD:C8:C9:32:B0:D8

X509v3 Authority Key Identifier:

keyid:66:32:4C:2C:D7:83:1E:EC:6C:0D:4D:DB:AA:3C:BD:C8:C9:32:B0:D8

**X509v3 Basic Constraints:**

**CA:FALSE**

Signature Algorithm: md5WithRSAEncryption

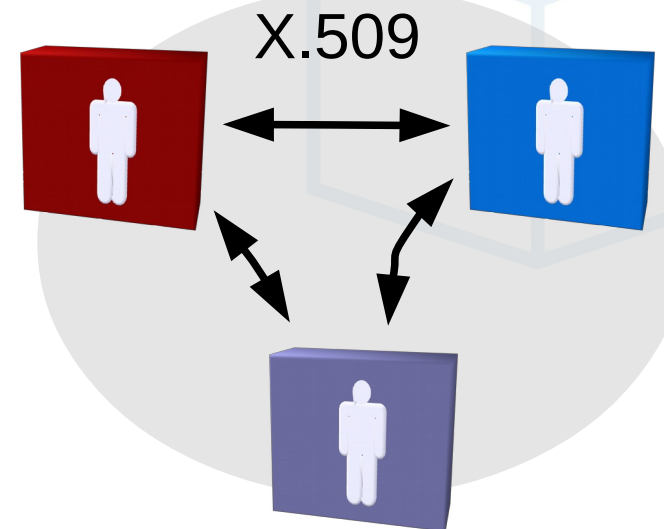
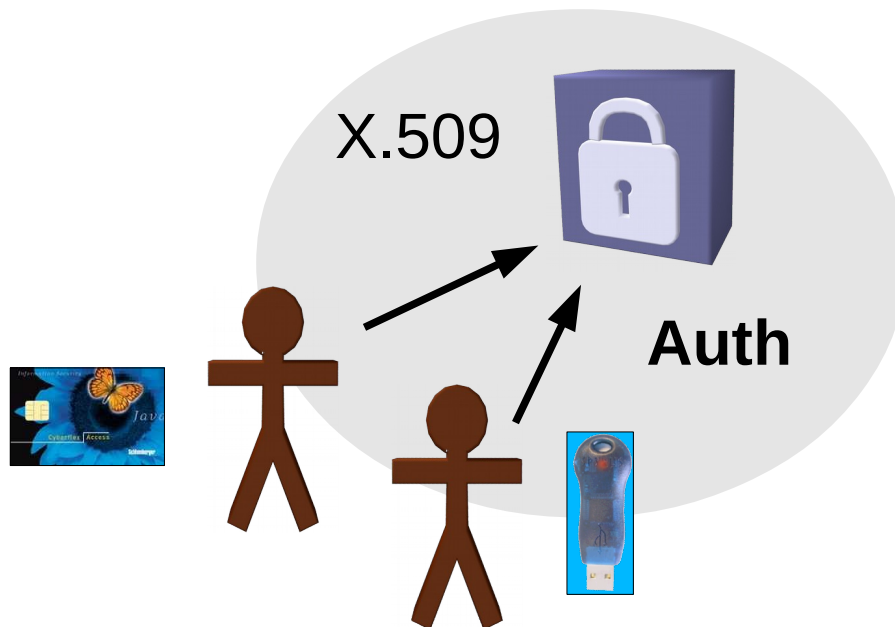
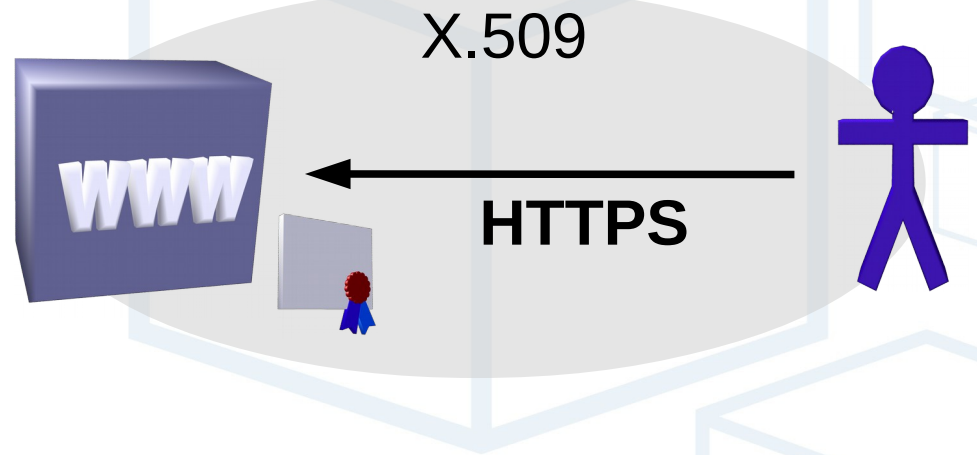
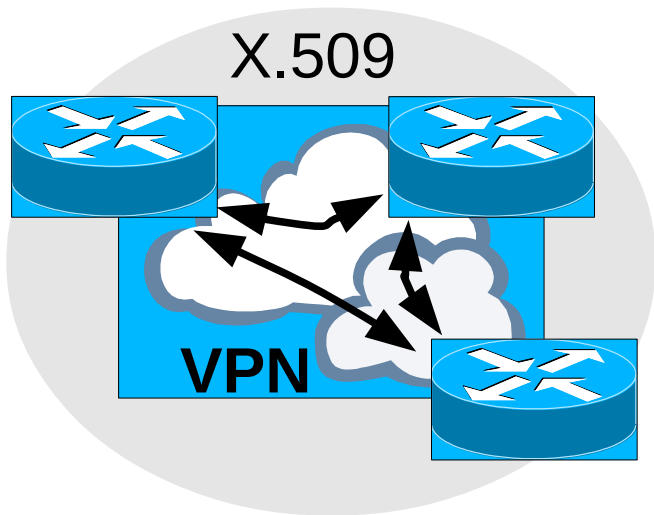
0a:eb:34:36:5f:37:fc:bf:df:13:6d:1e:ee:cd:cc:91:b3:e2:

d9:f9:33:21:28:a8:63:75:57:ba:8c:15:c5:ca:86:2f:14:64:

cc:dd:54:75:4f:ad:09:eb:ef:d4:b6:e0:ca:53:d1:

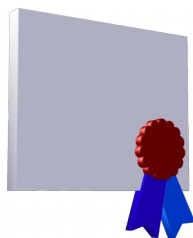
.....

# Kde sa PKI používa?

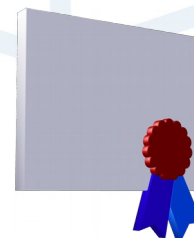


# Jedna Certifikační Autorita

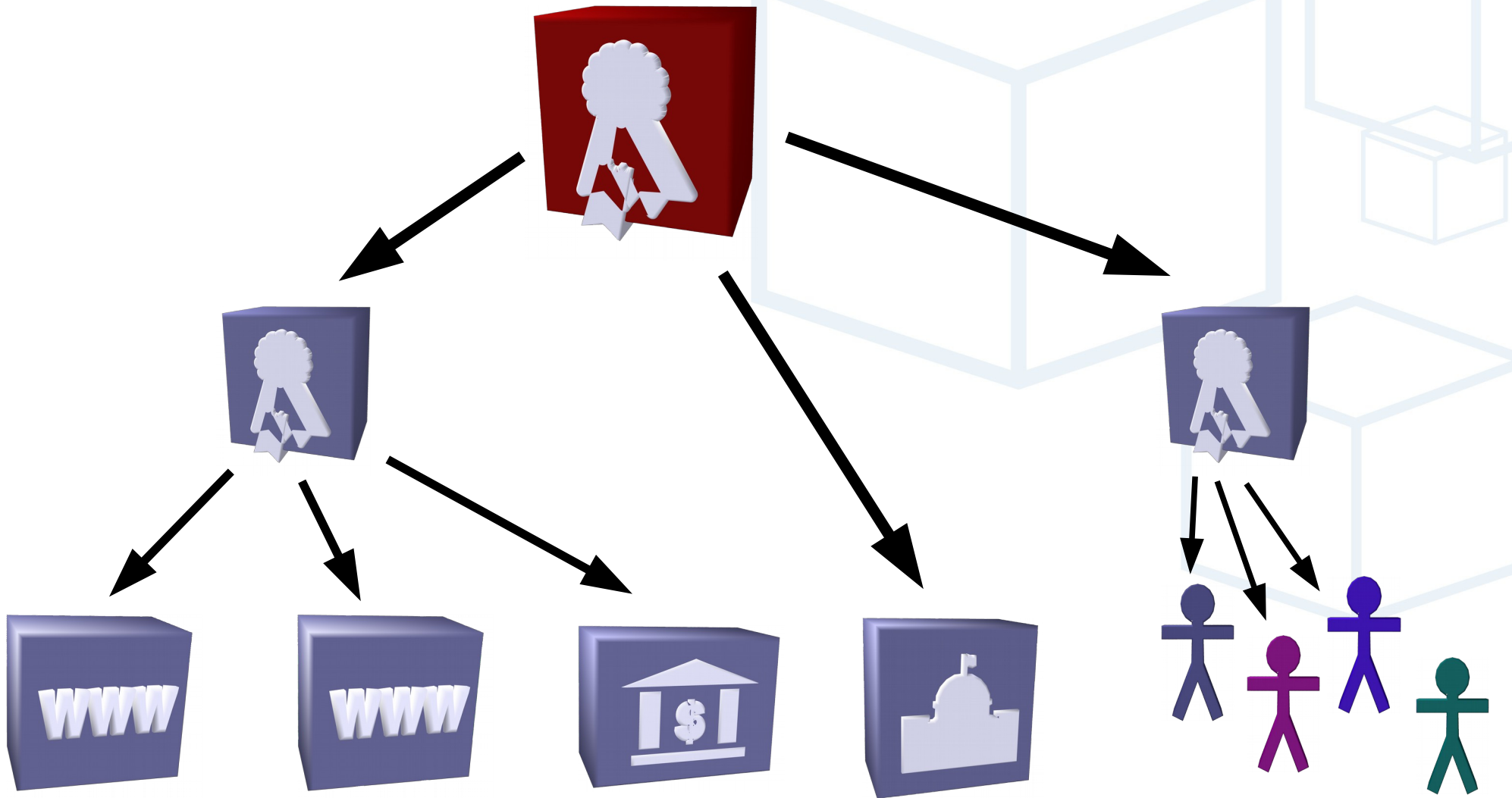
Alice



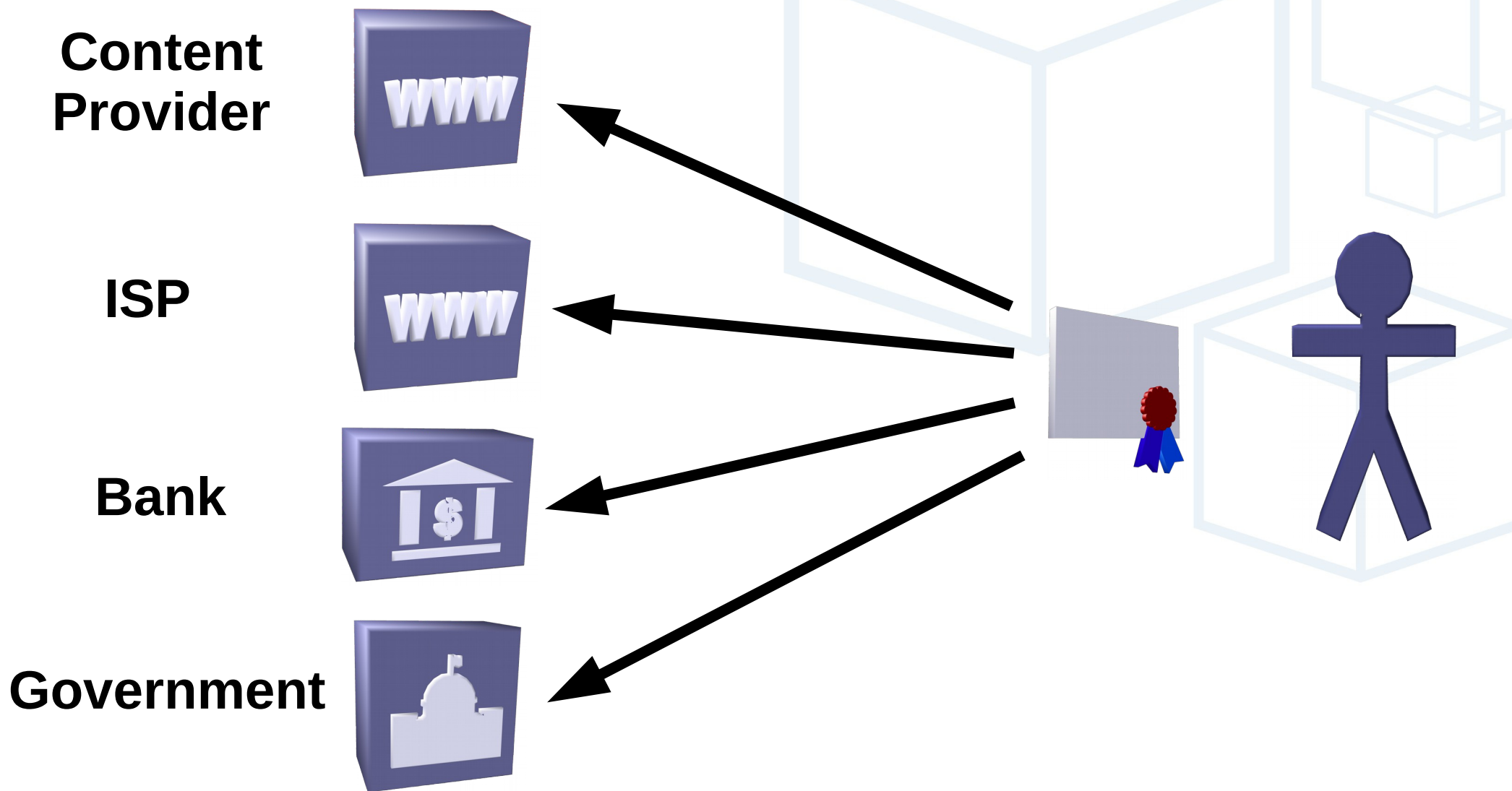
Bob



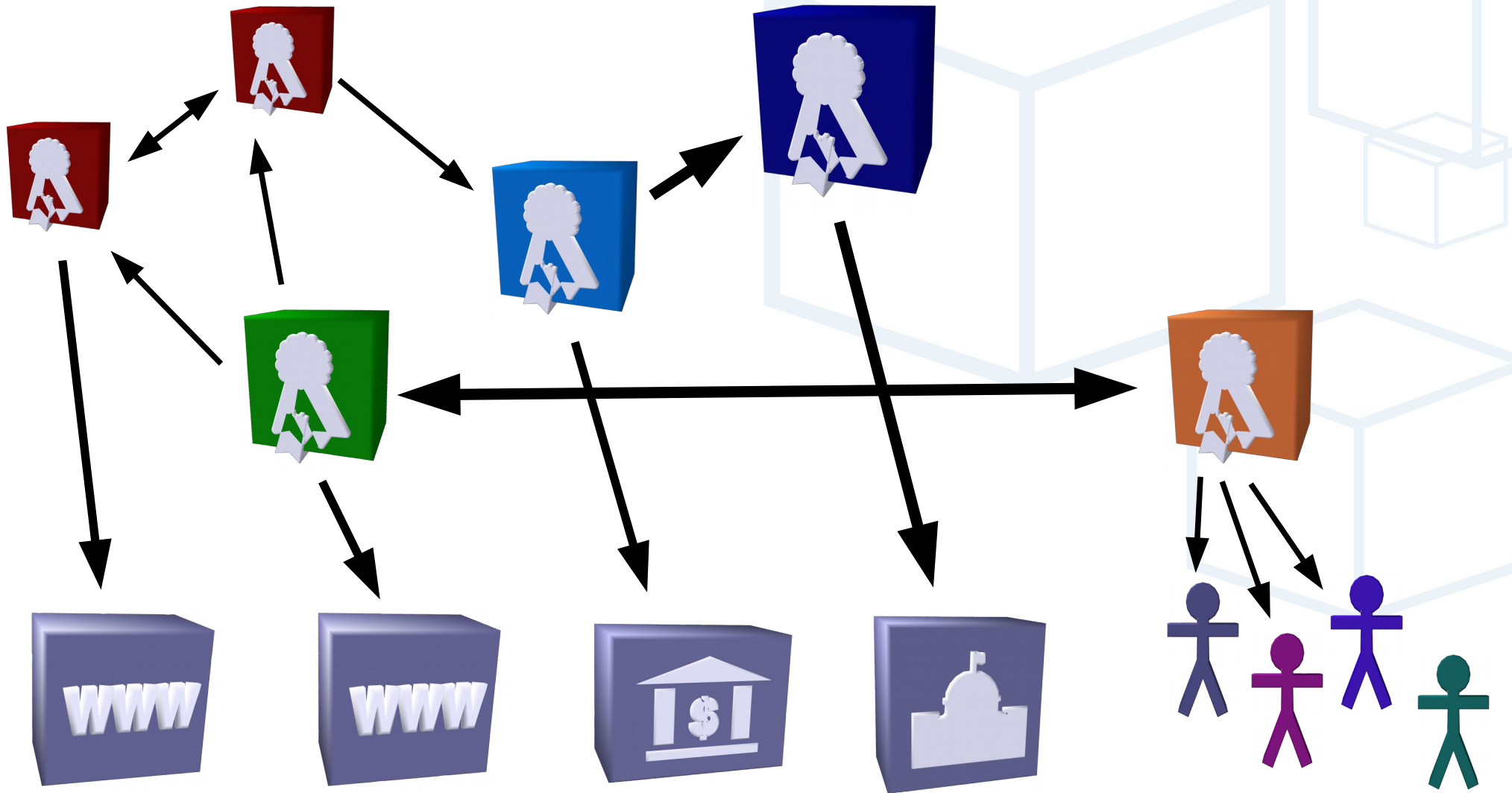
# Viac CA (Idea)



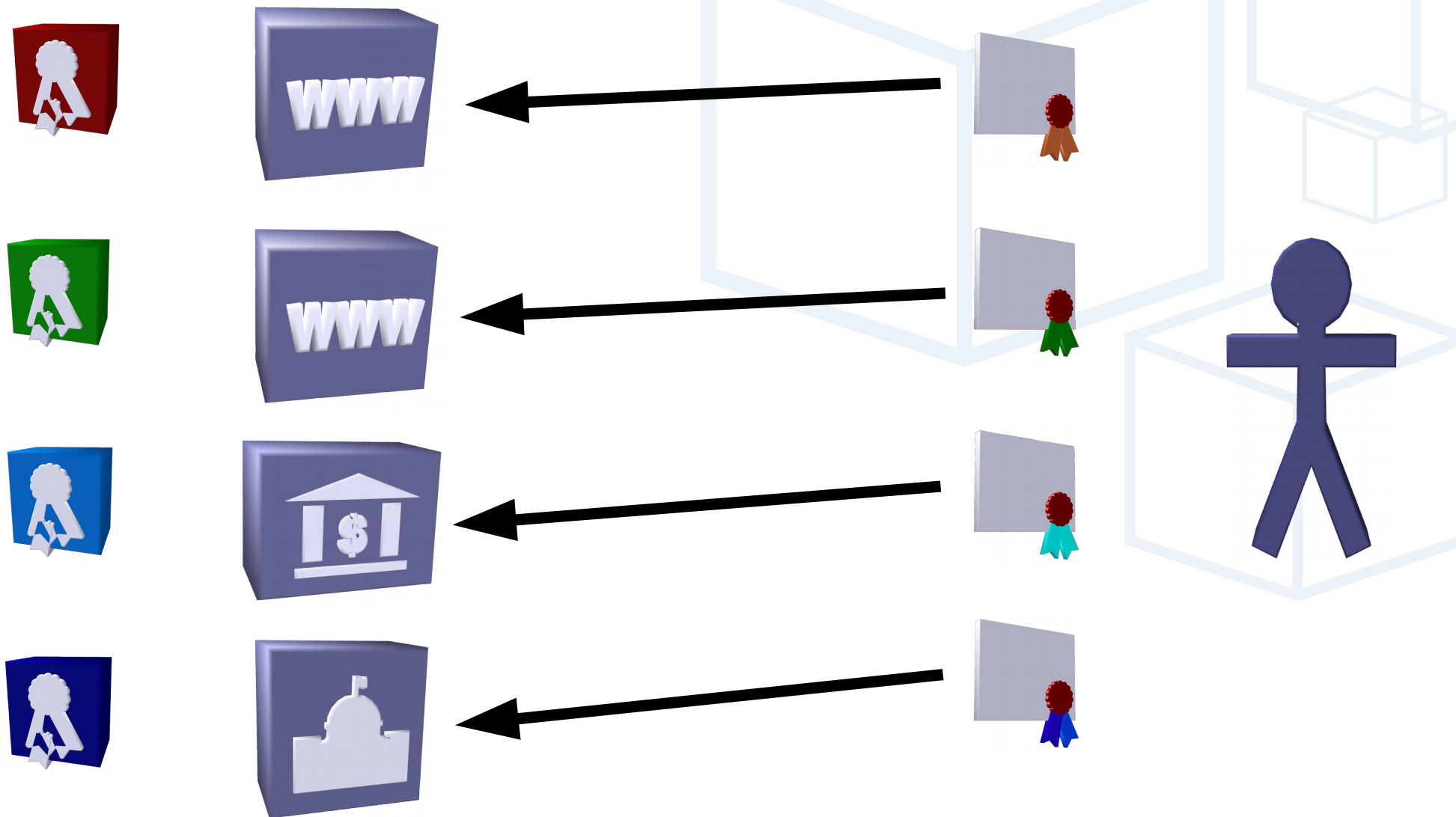
# Používateľský pohľad



# Viac CA (Realita)



# Používateľský pohľad



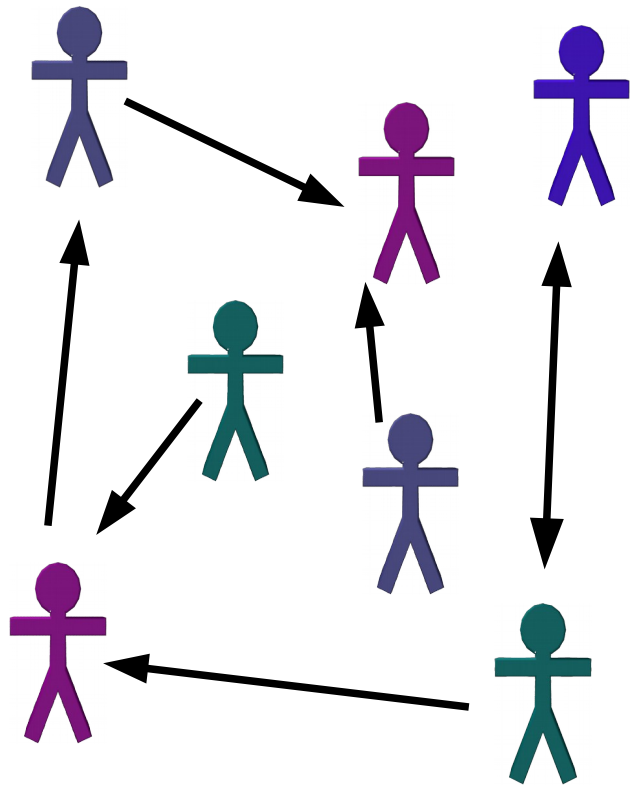


# Philip R. Zimmermann

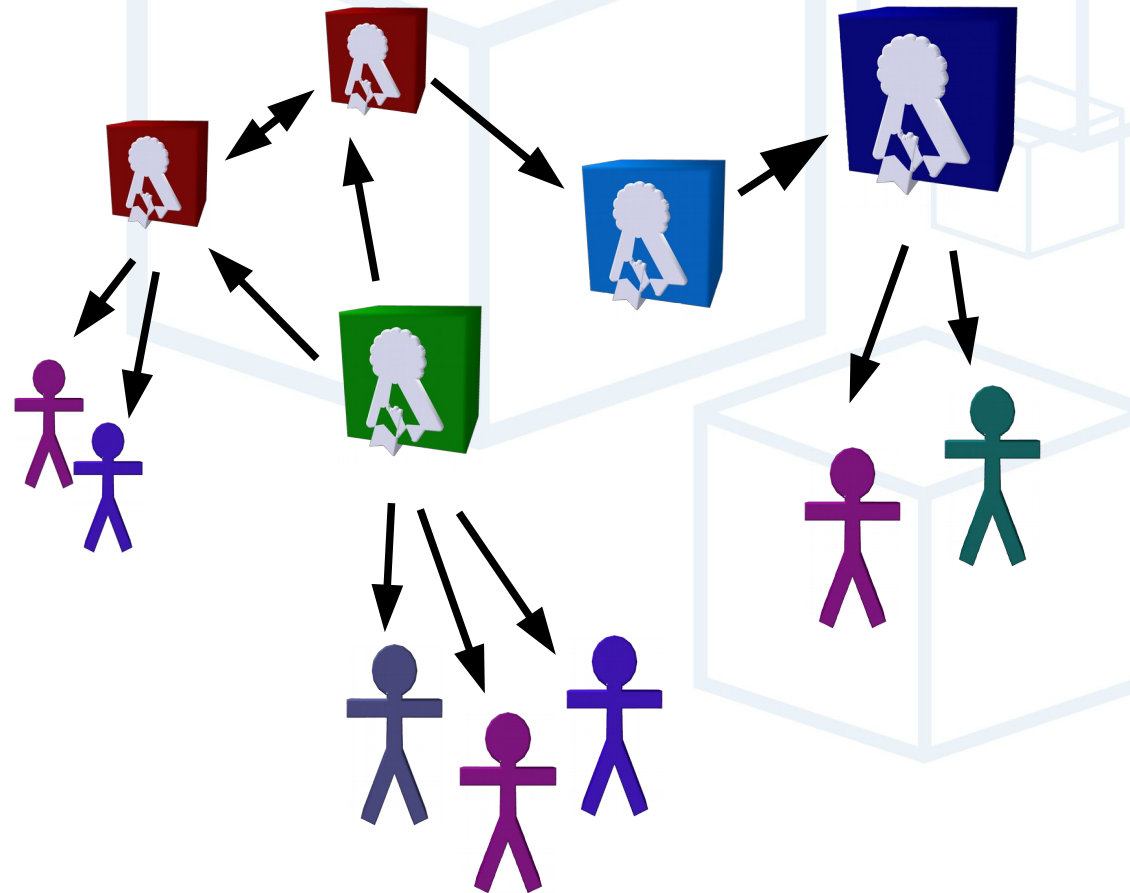
**Ja som to  
hovoril ...**



# Web of Trust vs Hybrid



**Web of Trust  
(PGP)**



**Hybrid  
(X.509)**

# Ďalšie PKI problémy

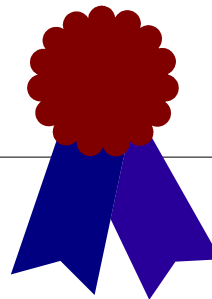
cn=Radovan Semančík

uid=rsemancik

guid=753e472xs47321

rc=030319/7032

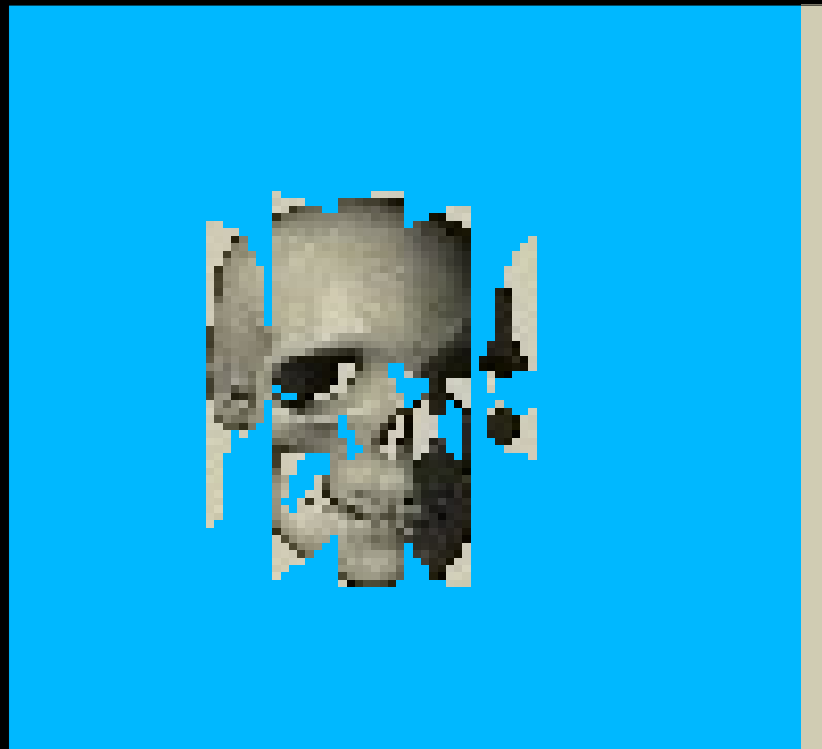
?

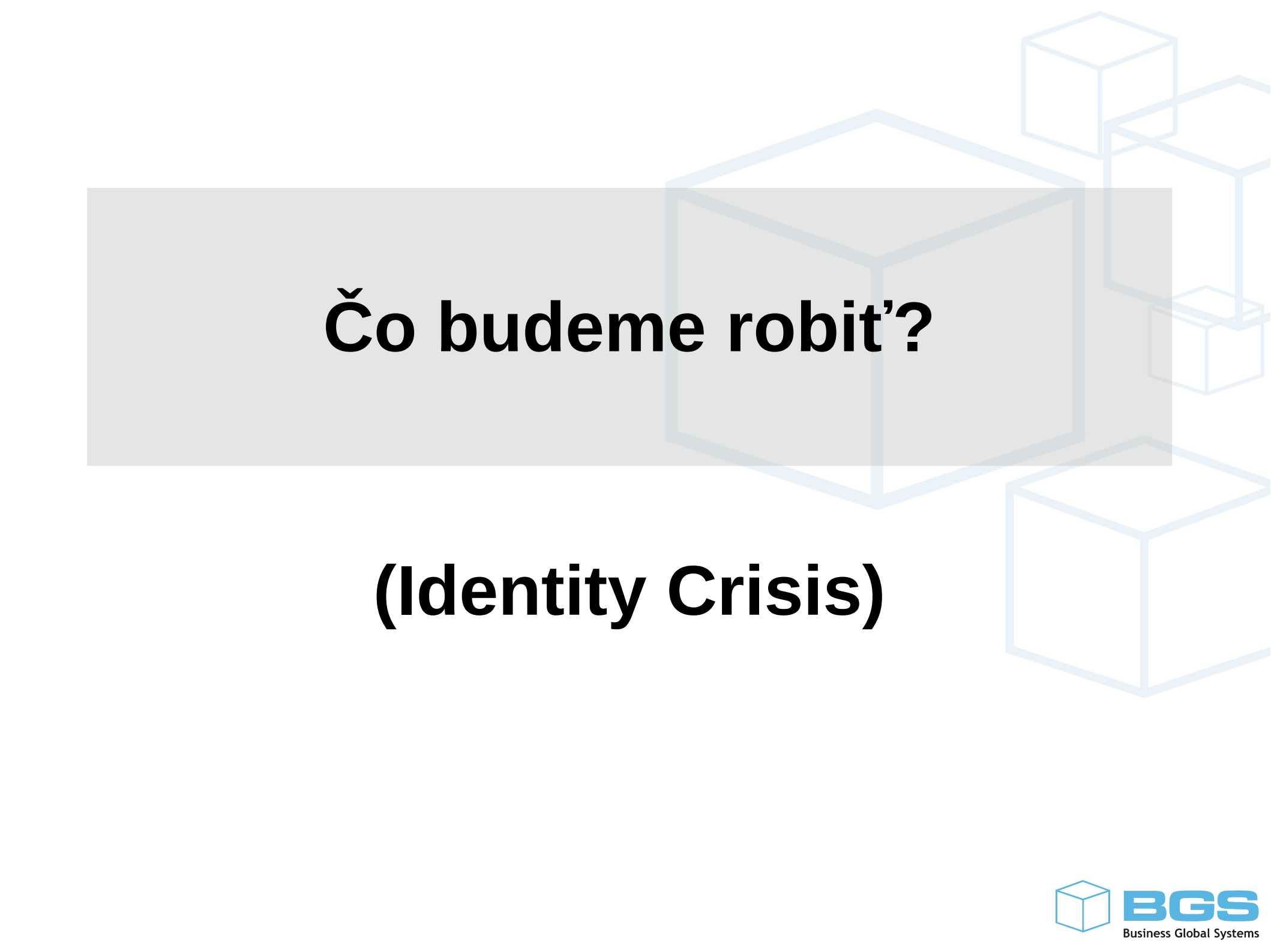


- Problémy:
- Súkromie
- Interoperability
- Access Control
- Priviléžia, Role



**PKI or not PKI?**  
That's the question ...





**Čo budeme robiť?**

**(Identity Crisis)**

# Identity

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

WordNet

Language  
Locality



SE35758423



Financial records  
Health records

rsemancik

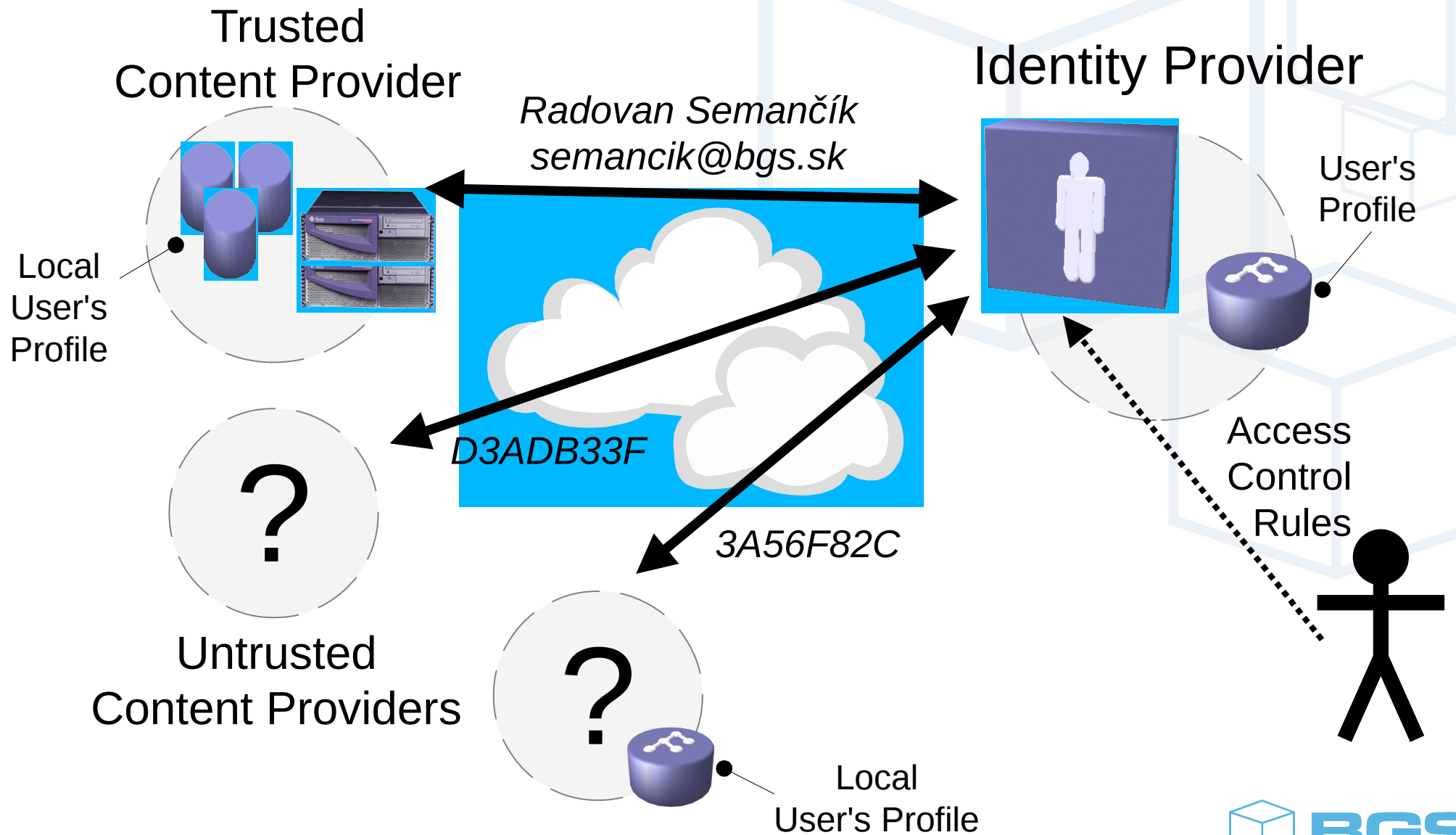


Shopping preferences  
Travel preferences

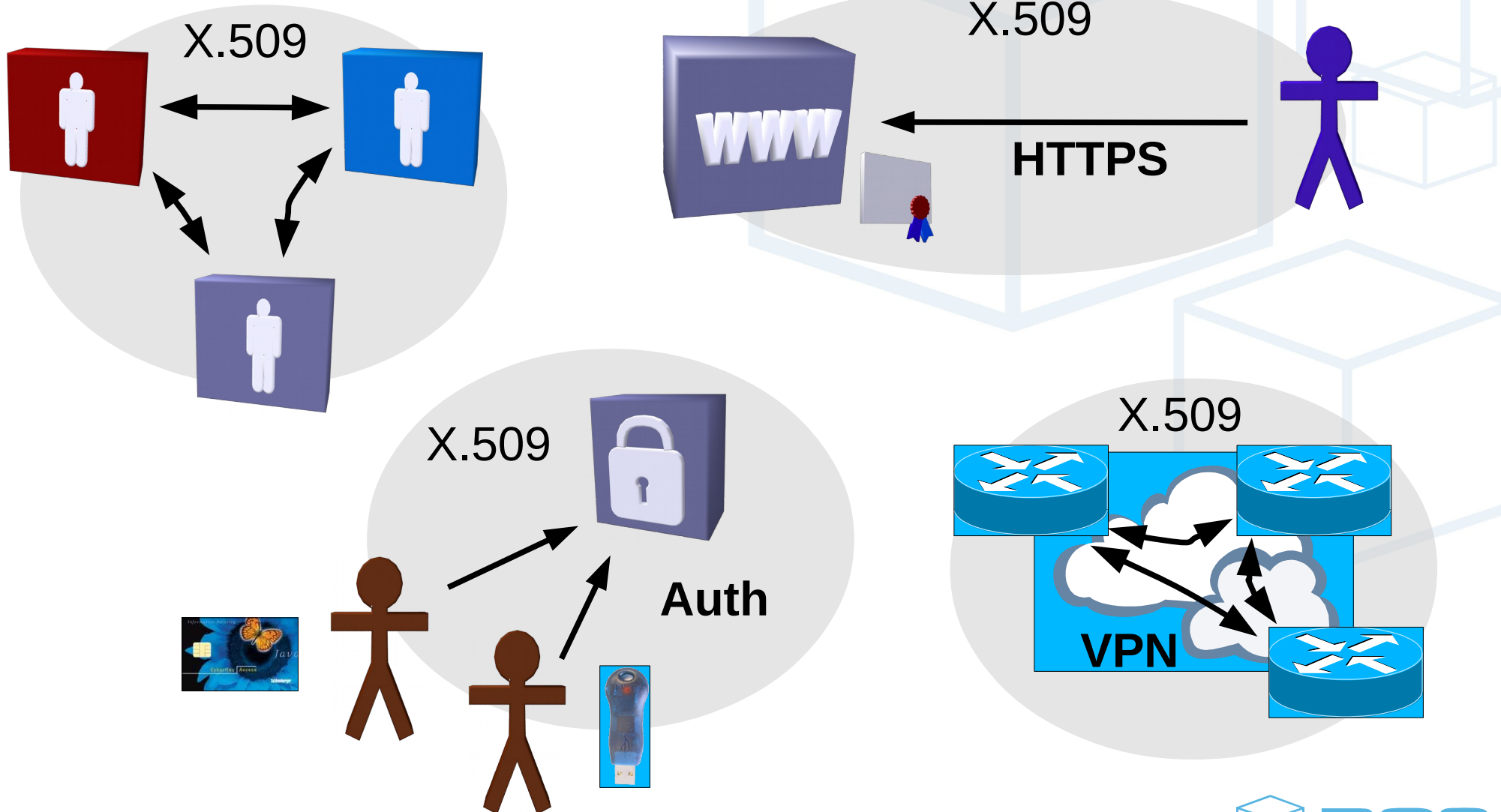
Title, Role  
Org. membership

Radovan Semančík

# Identity Management

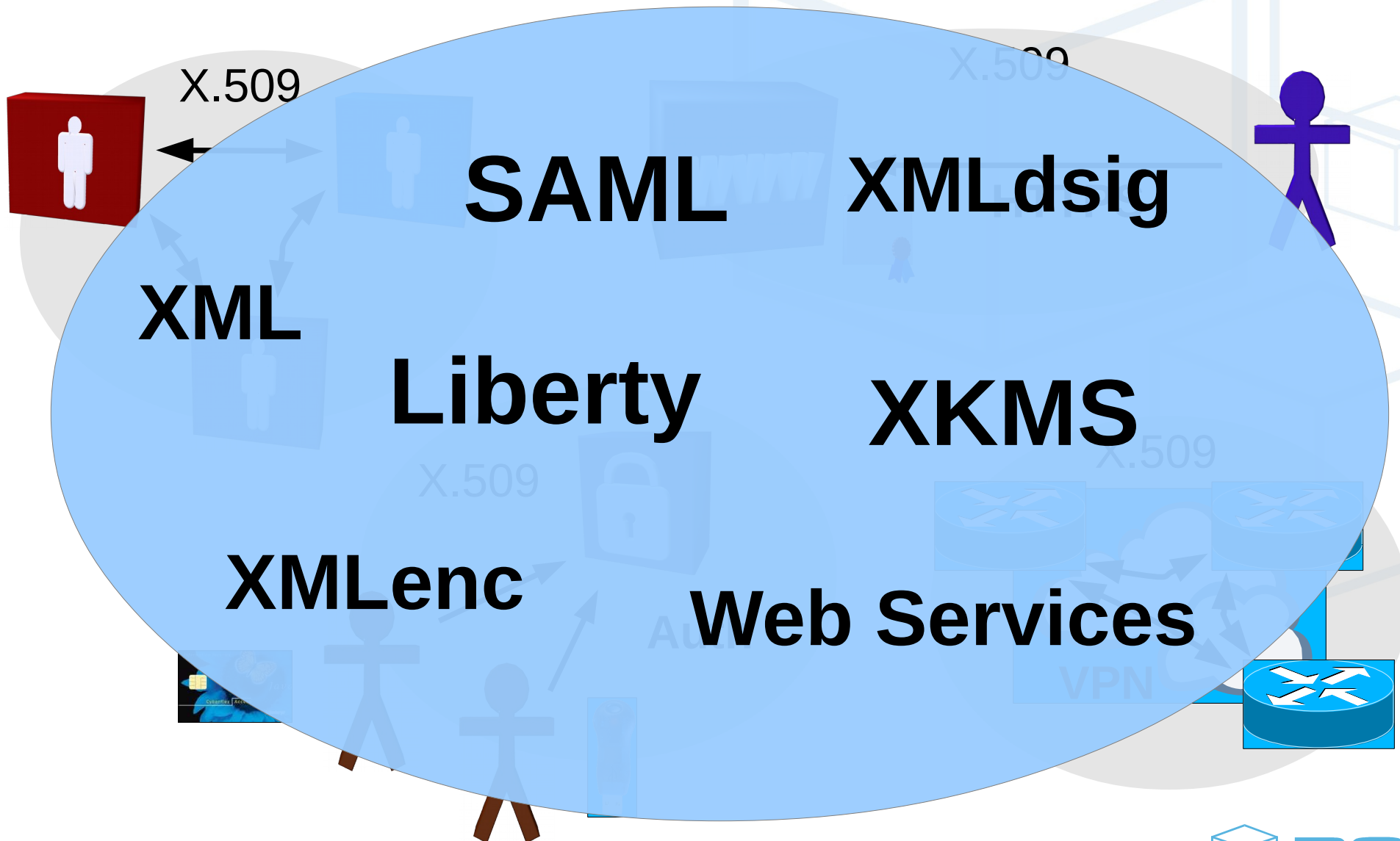


# X.509 PKI nie je úplne zlá





# XML-based “PKI”



# Questions?



Thank you ...

**Ing. Radovan Semančík**  
Chief Information Officer

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

[semancik@bgs.sk](mailto:semancik@bgs.sk)

