Digital Identity

SkLUG Linux Weekend
Október 2002, Žilina

Ing. Radovan Semančík

BGS
Business Global Systems

Agenda

- Čo?
- Prečo?
- Ako?
- A čo teraz?
- A vôbec ...

BGS
Business Global Systems

Čo?

- Digital Identity
  - Network Identity
  - Internet Identity
  - Federated Identity
  - ...
- Bezpečnosť ako ju nepoznáme
- Budúcnosť ….

BGS
Business Global Systems

Agenda

- Čo?
- Prečo?
- Ako?
- A čo teraz?
- A vôbec ...

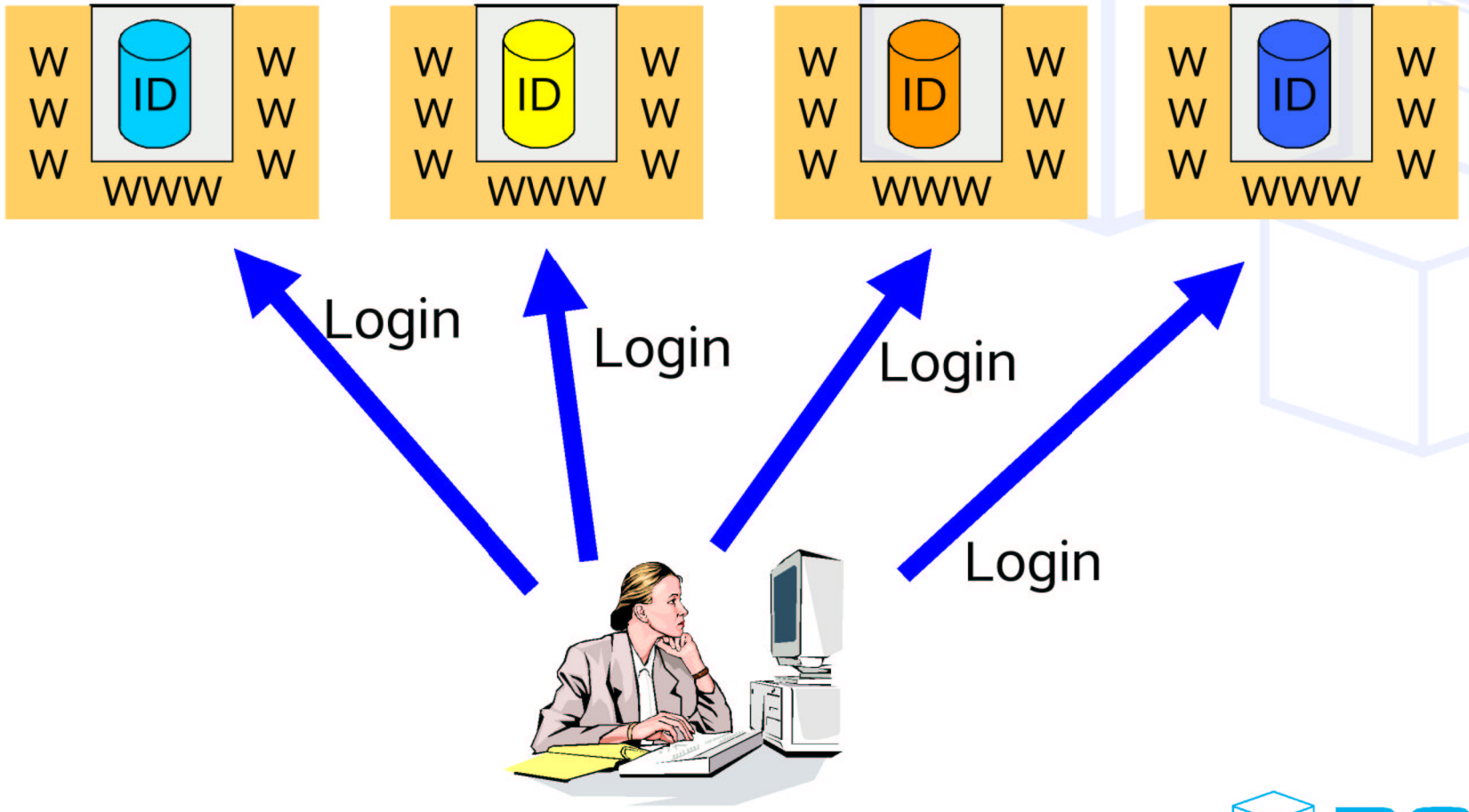
BGS
Business Global Systems

Ako to celé začalo?

- In the beginning, there was a (pass)word
- Prvé heslo: UNIX
- Druhé heslo: NT domain
- Tretie heslo: Internet site
- Štvrté heslo: Intranet site
- Piate heslo: Ďalší Internet site
- Šieste heslo: ešte ďalší Internet site

BGS
Business Global Systems

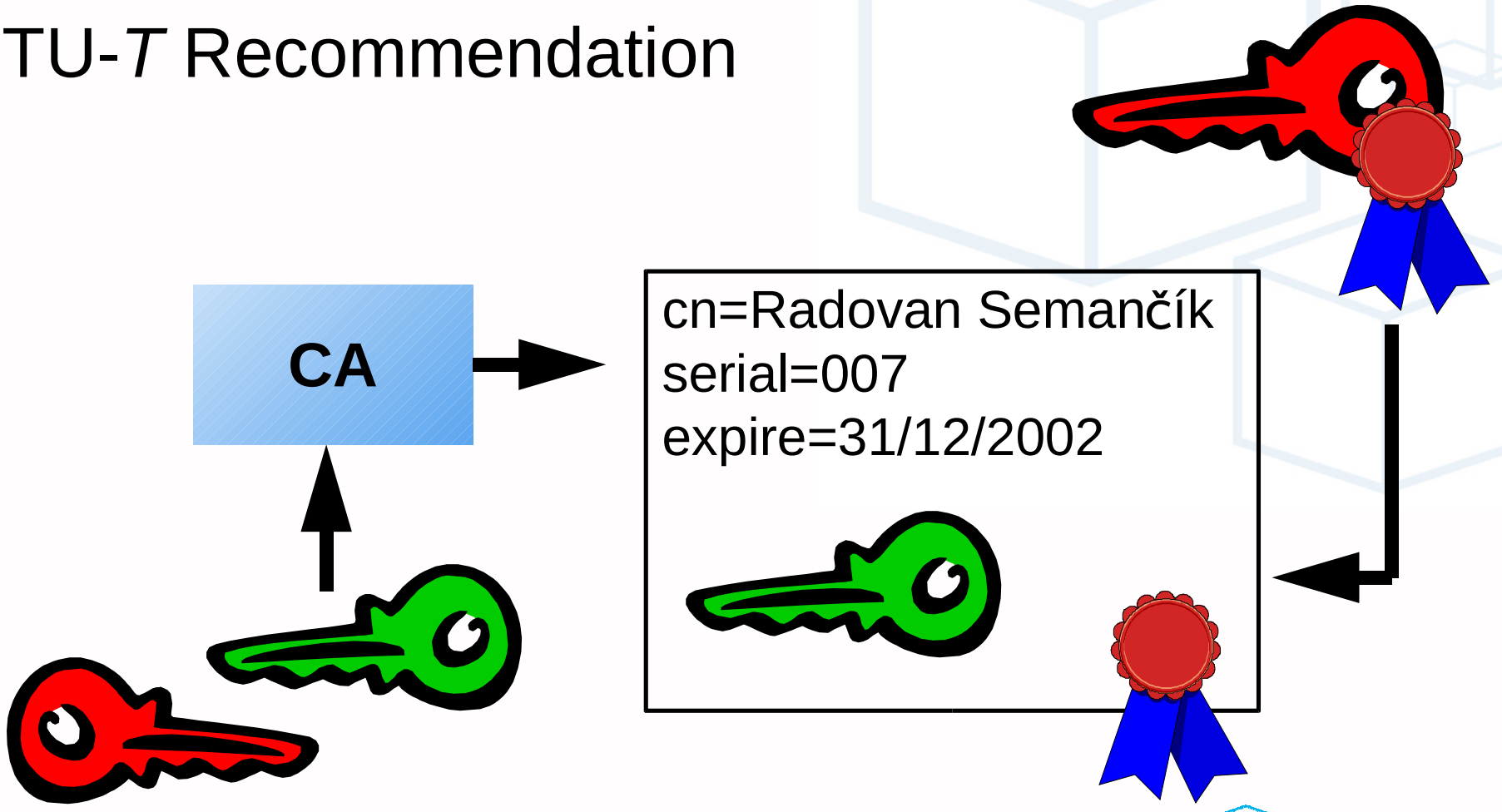
Auth, Autz & WWW



BGS
Business Global Systems

X.509 digitálne certifikáty

ITU-*T* Recommendation



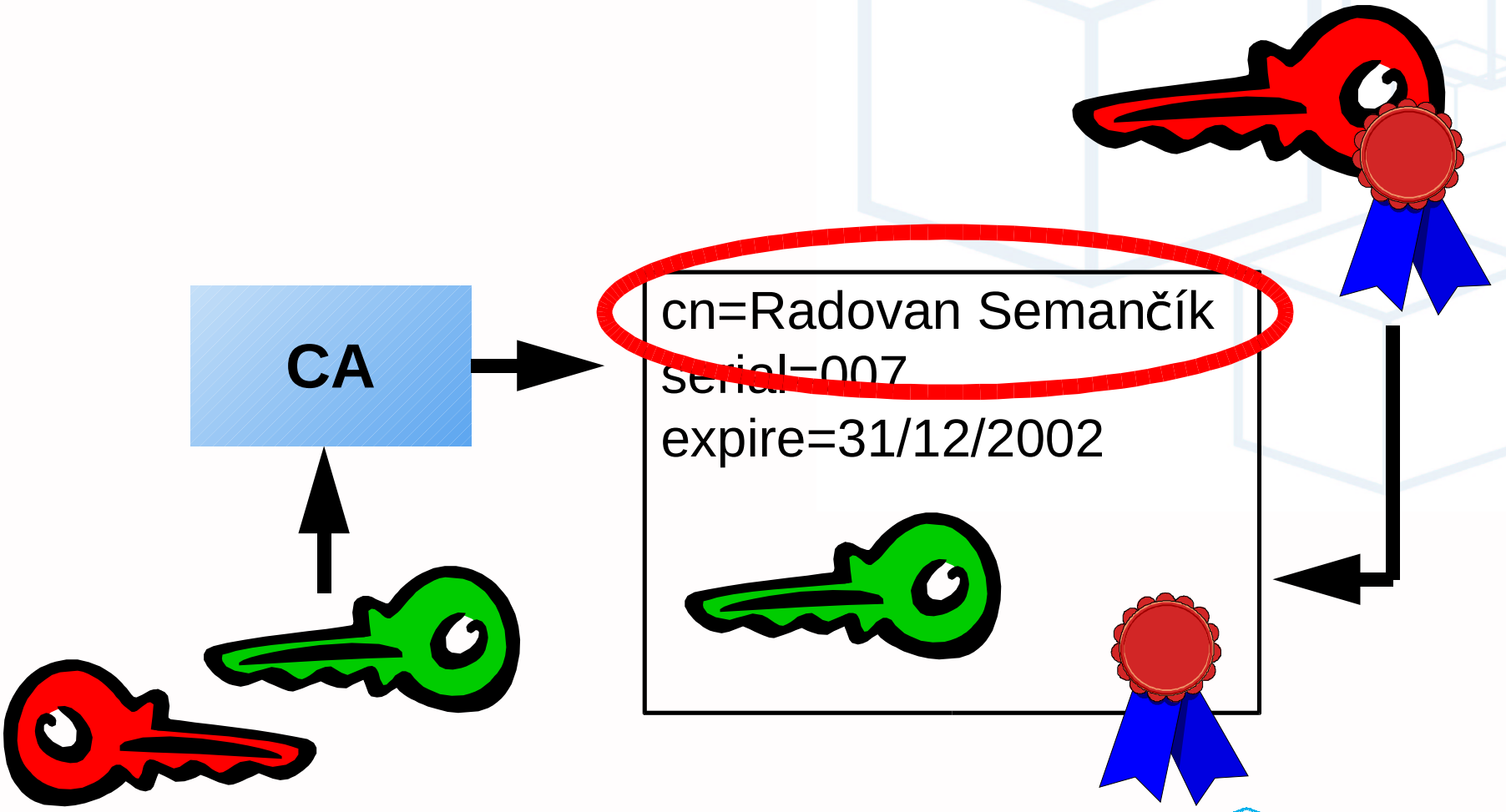
BGS
Business Global Systems

X.509 certificate

```
Version: 3 (0x2)
Serial Number: 1 (0x1)
Signature Algorithm: md5WithRSAEncryption
Issuer: C=US, O=Snake Oil, Ltd, OU=Certificate Authority, CN=Snake Oil CA
Validity
     Not Before: Oct 21 18:21:51 1999 GMT
     Not After : Oct 20 18:21:51 2001 GMT
Subject: C=US, O=Snake Oil, Ltd, OU=Webserver Team, CN=www.snakeoil.dom
Subject Public Key Info:
     Public Key Algorithm: rsaEncryption
     RSA Public Key: (1024 bit)
     Modulus (1024 bit):
          00:b9:e7:84:68:.....
     Exponent: 65537 (0x10001)
X509v3 extensions:
     X509v3 Subject Alternative Name: email:www@snakeoil.dom
     Netscape Comment: mod_ssl custom server certificate
     Netscape Cert Type: SSL Server
Signature Algorithm: md5WithRSAEncryption
     7a:31:1b:18:19:.....
```

BGS
Business Global Systems

X.509 digitálne certifikáty



BGS
Business Global Systems

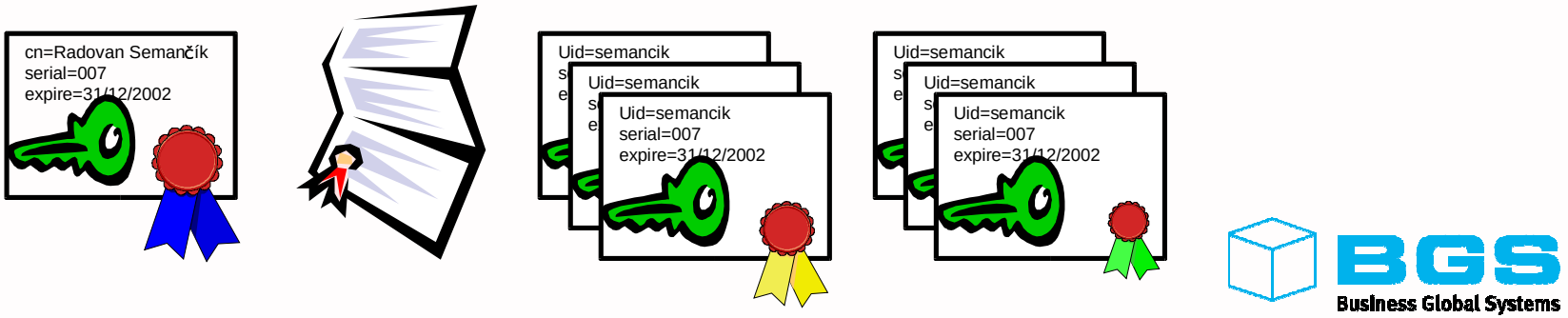
X.500 Distinguished Name

- cn=Radovan Semancik, o=bgs, c=sk
- uid=semancik, ou=people, o=bgs, c=sk
- dc=semancik, dc=bgs, dc=sk
- uid=semancik, o=bgs.sk

BGS
Business Global Systems

X.500 Distinguished Name

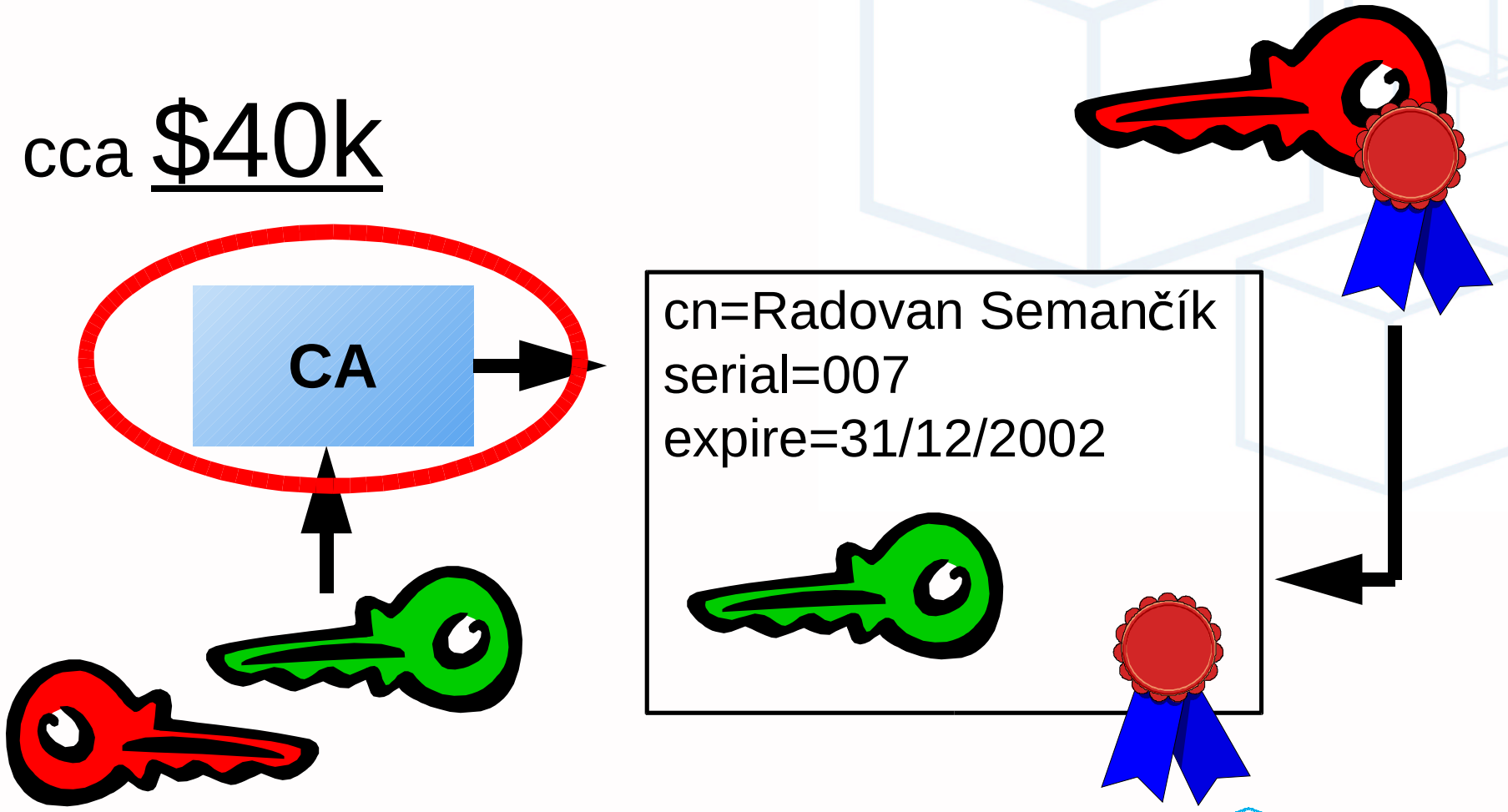
- uid=semancik, ou=people, o=bgs, c=sk
- cn=gildir, o=sklug, c=sk
- nick=Gildir, dc=silcnet, dc=org
- cn=gildir, dc=perlmonks.org
- Uid=gldr, o=overcrowded-site
- Uid=rse, ou=partner, o=bigcompany.com



BGS
Business Global Systems

X.509 digitálne certifikáty

cca $40k



BGS
Business Global Systems

Certifikačná autorita

- Overovanie totožnosti
- Vydávanie certifikátov
- Zneplatňovanie certifikátov
- Udržovanie evidencie

- ... a to všetko platí používateľ ($$$)

BGS
Business Global Systems

A čo PGP?

- Nerieši problém – Ako overím kľúč:

  looser@whatTheHell.com
- Prečo by som mal veriť Ferovi, ktorý tvrdí, že jeho brata psa kamarát má pána, ktorý v bare stretol kolegu a overil jeho verejný kľúč?
- PGP vhodné pre malé nasadenie, ale nie globálne

BGS
Business Global Systems

Sci-fi … a stále problémy

- Mám len dve identity = dva certifikáty
  - **uid=semancik, ou=people, o=bgs, c=sk**
  - **cn=gildir, o=community, c=org**

- Dám do certifikátu email? – SPAM
- Dám do certifikátu adresu? - shopping
- Dám do certifikátu rodné číslo? - gov

BGS
Business Global Systems

Registračné formuláre

- First name:
- Last name:
- Title:
- Company name:
- Address:
- City:
- ZIP:
- Country:
- E-mail address:
- Work position:
- Would you like to receive product updates?

Grrrrrrrrrr!

BGS
Business Global Systems

Agenda

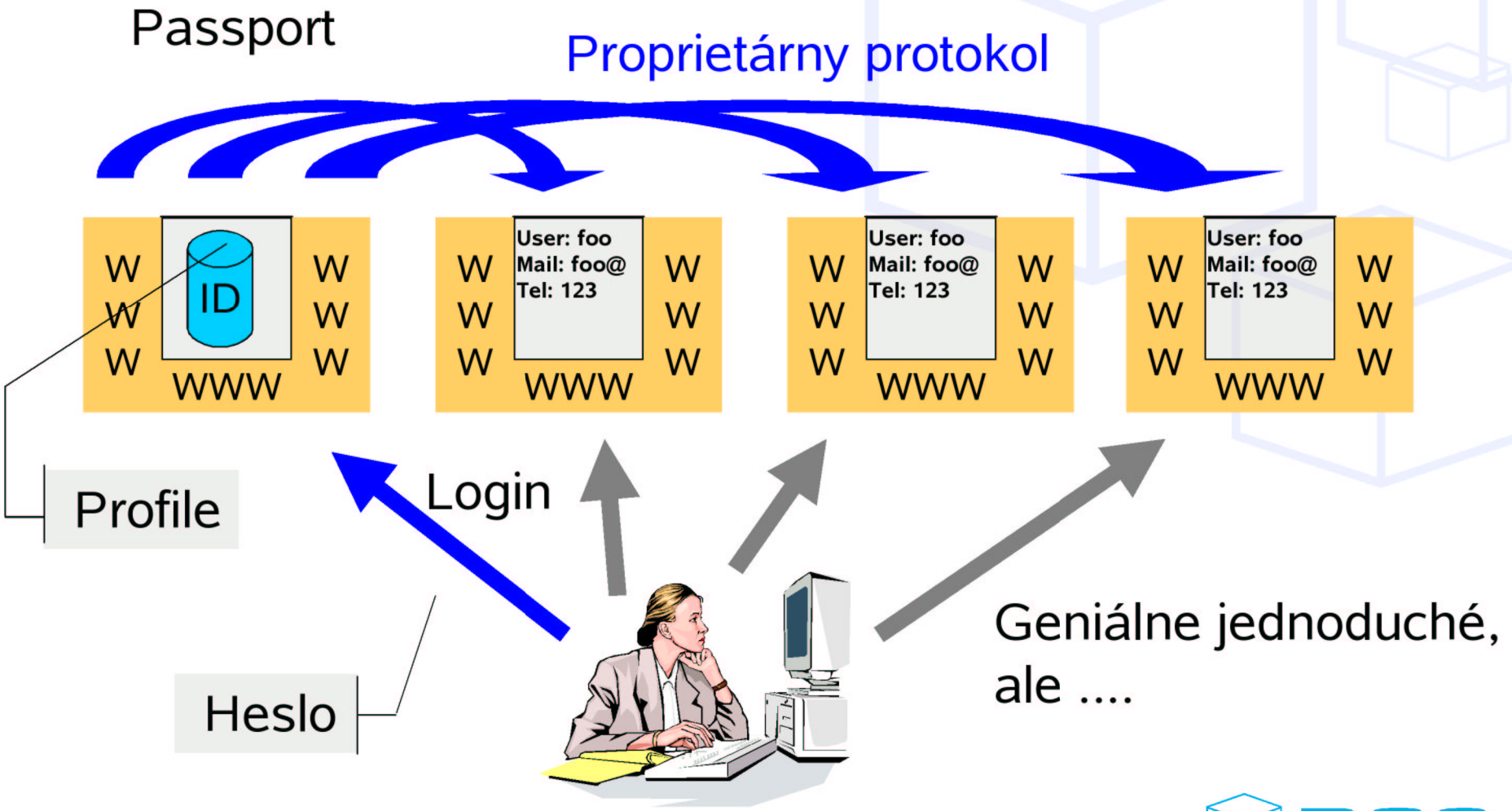
- Čo?
- Prečo?
- Ako?
- A čo teraz?
- A vôbec ...

BGS
Business Global Systems

Ako?

BGS
Business Global Systems

Digital Identity (začiatky)



BGS
Business Global Systems

... ale

- **Včera:** Realname, adresa, email, telefón
- **Dnes:** čísla kreditiek, nákupné preferencie
- **Zajtra:** stav účtu, dátum narodenia, národnoť, rasa, sexuálna orientácia, ...

- Where do you want to go tomorrow?

BGS
Business Global Systems

Agenda

- Čo?
- Prečo?
- Ako?
- A čo teraz?
- A vôbec ...

BGS
Business Global Systems

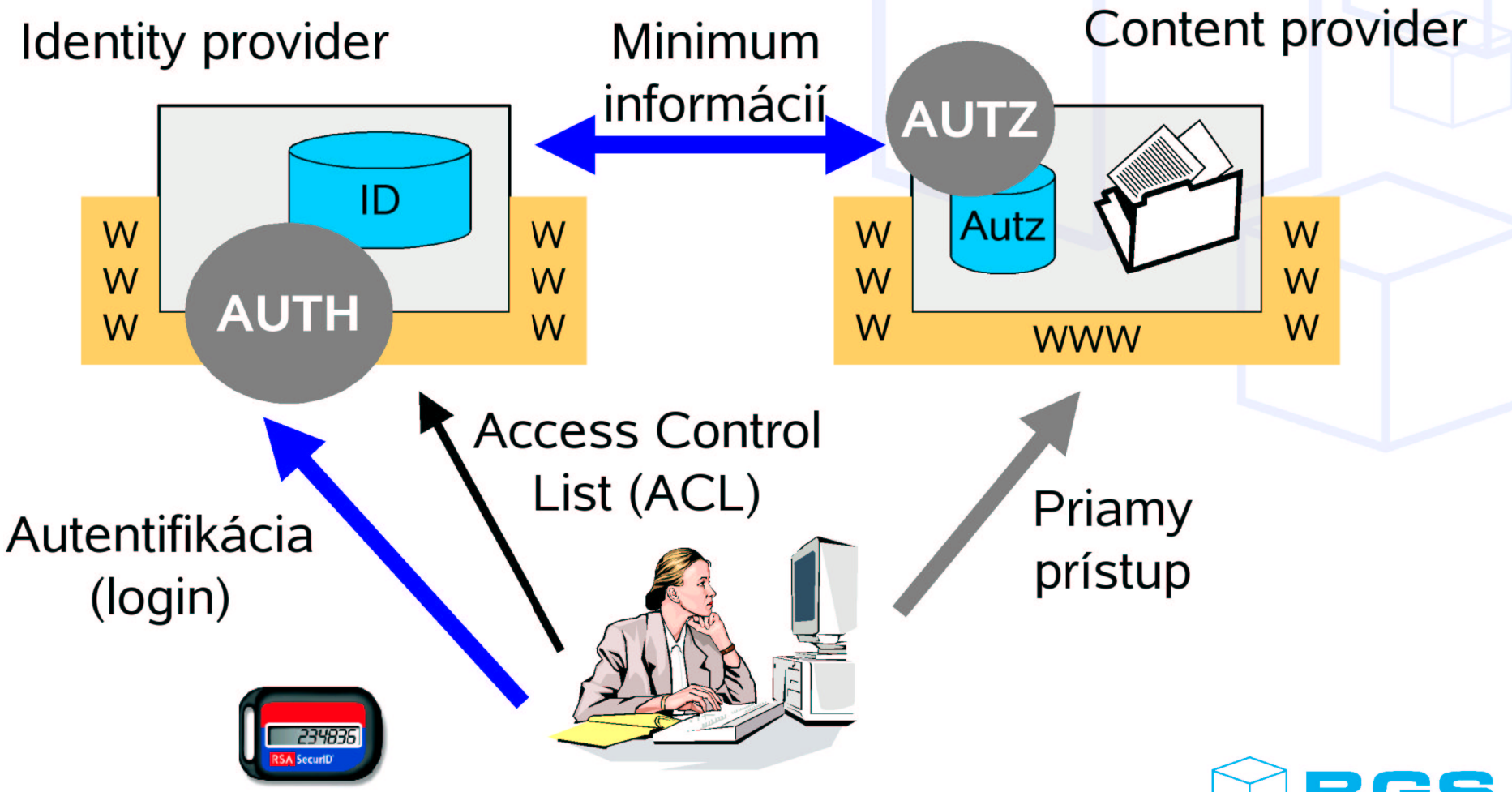
Sloboda výberu

Kto bude Identity Provider?

- Moja banka
- Môj zamestnávateľ
- Môj ISP
- ... niekto komu dôverujem

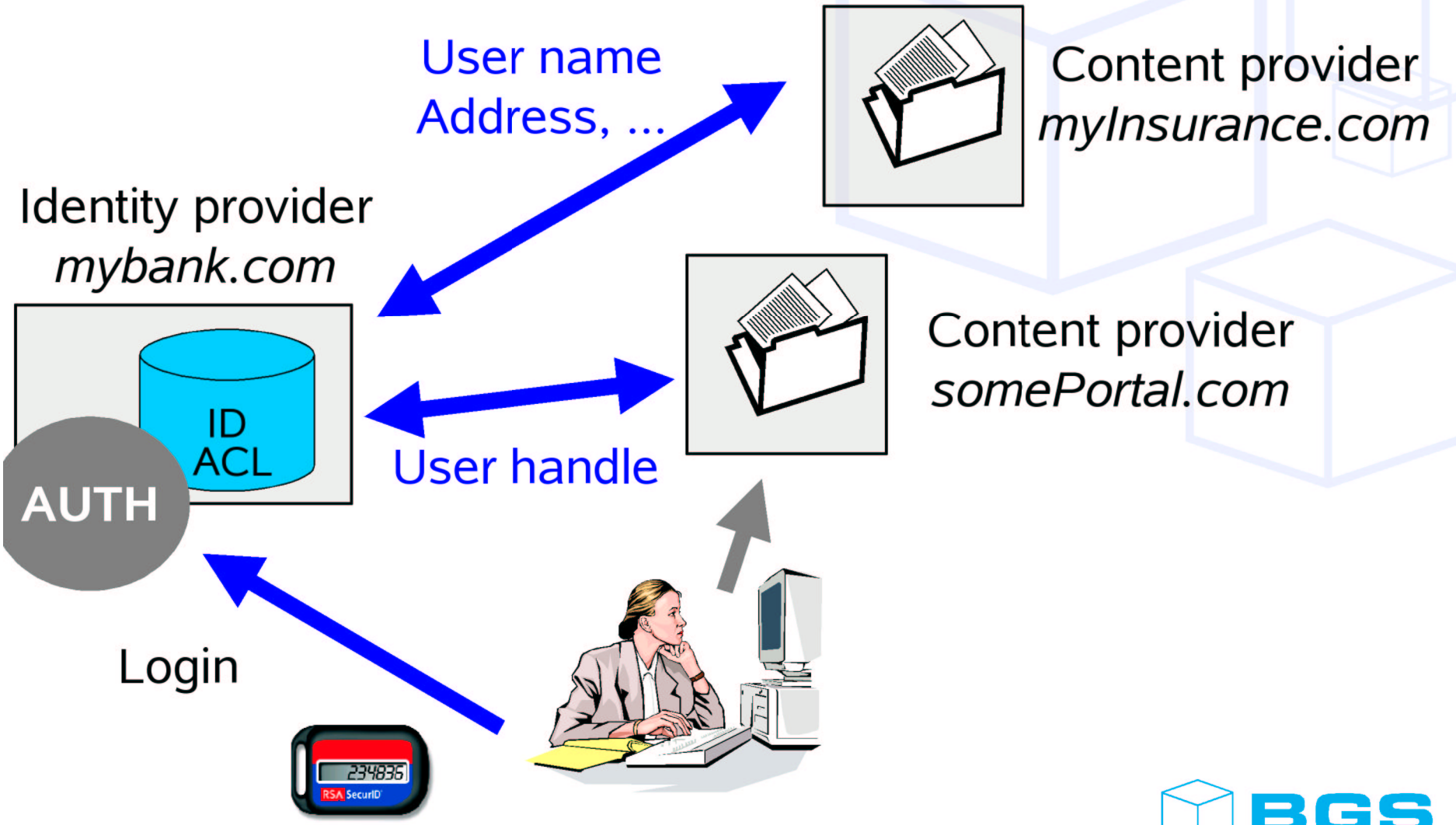
BGS
Business Global Systems

Identity provider



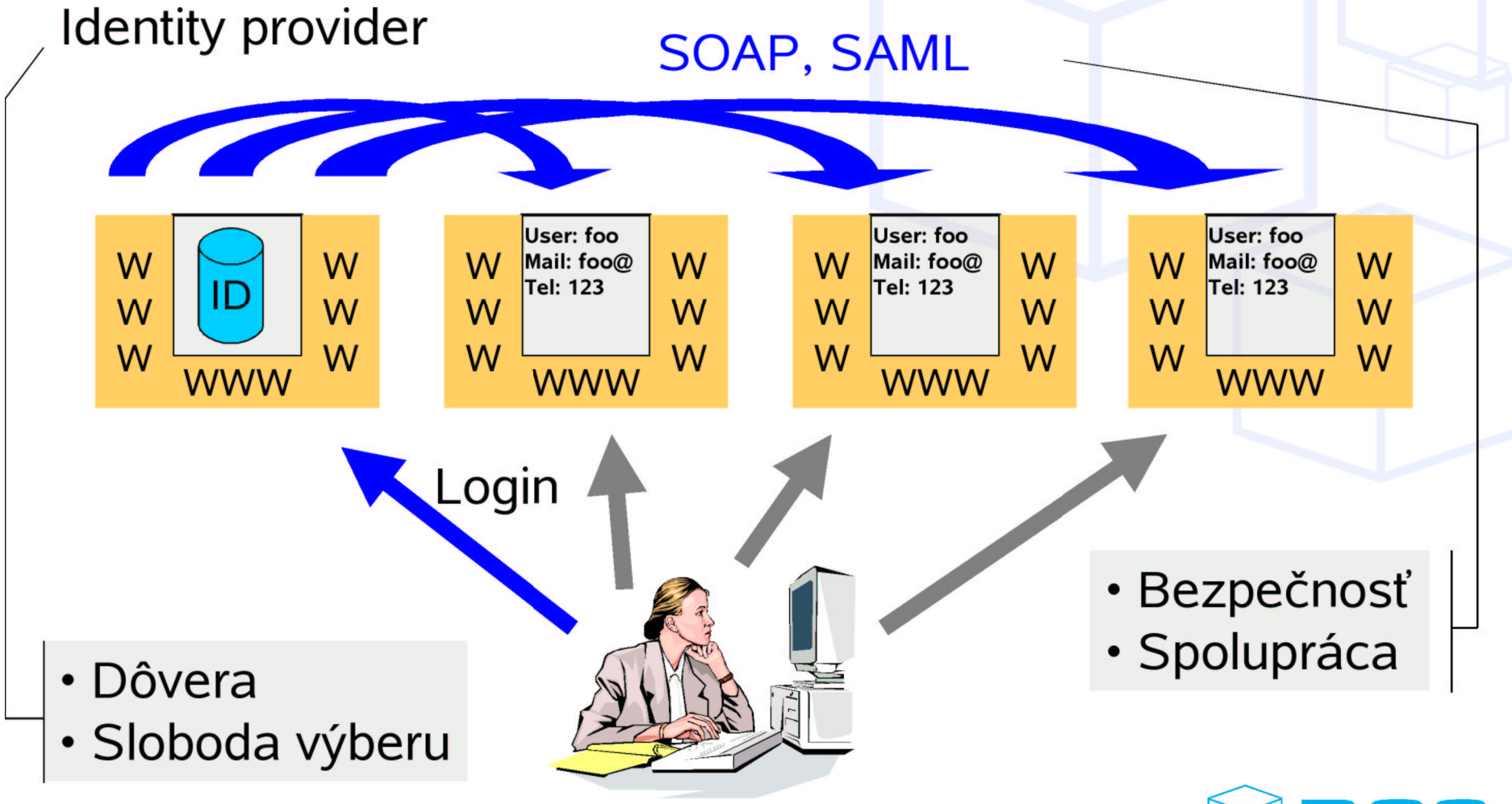
BGS
Business Global Systems

Identity provider



BGS
Business Global Systems

Digital Identity (dnes)



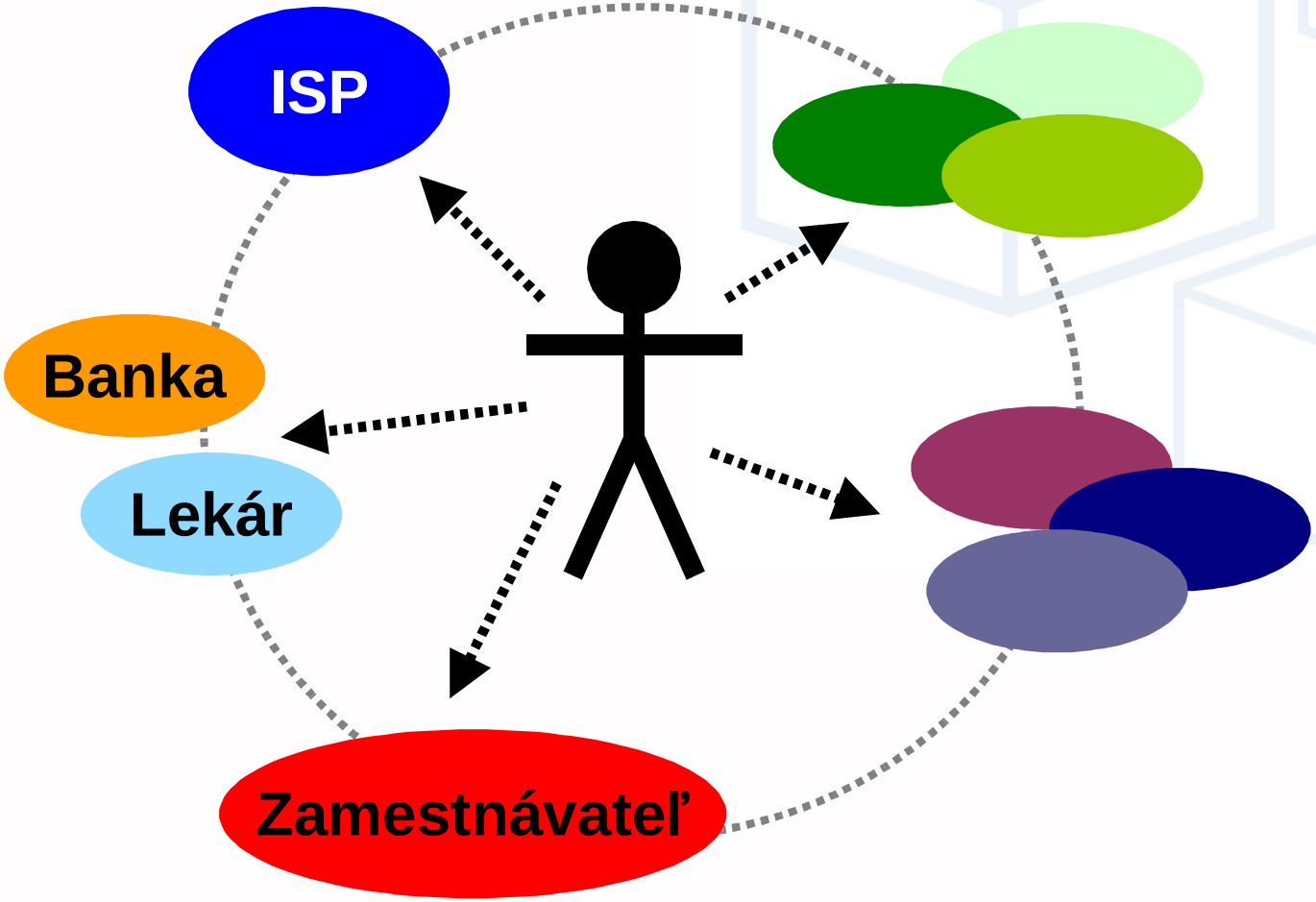
BGS
Business Global Systems

Digital Identity

- WWW aplikácie
  - Single Sign-On
  - Používateľské profily
- Web services
  - WS-Security
  - Bezpečné transakcie
- A čo PKI?
  - Na úrovni SAML
  - Autentifikácia používateľa

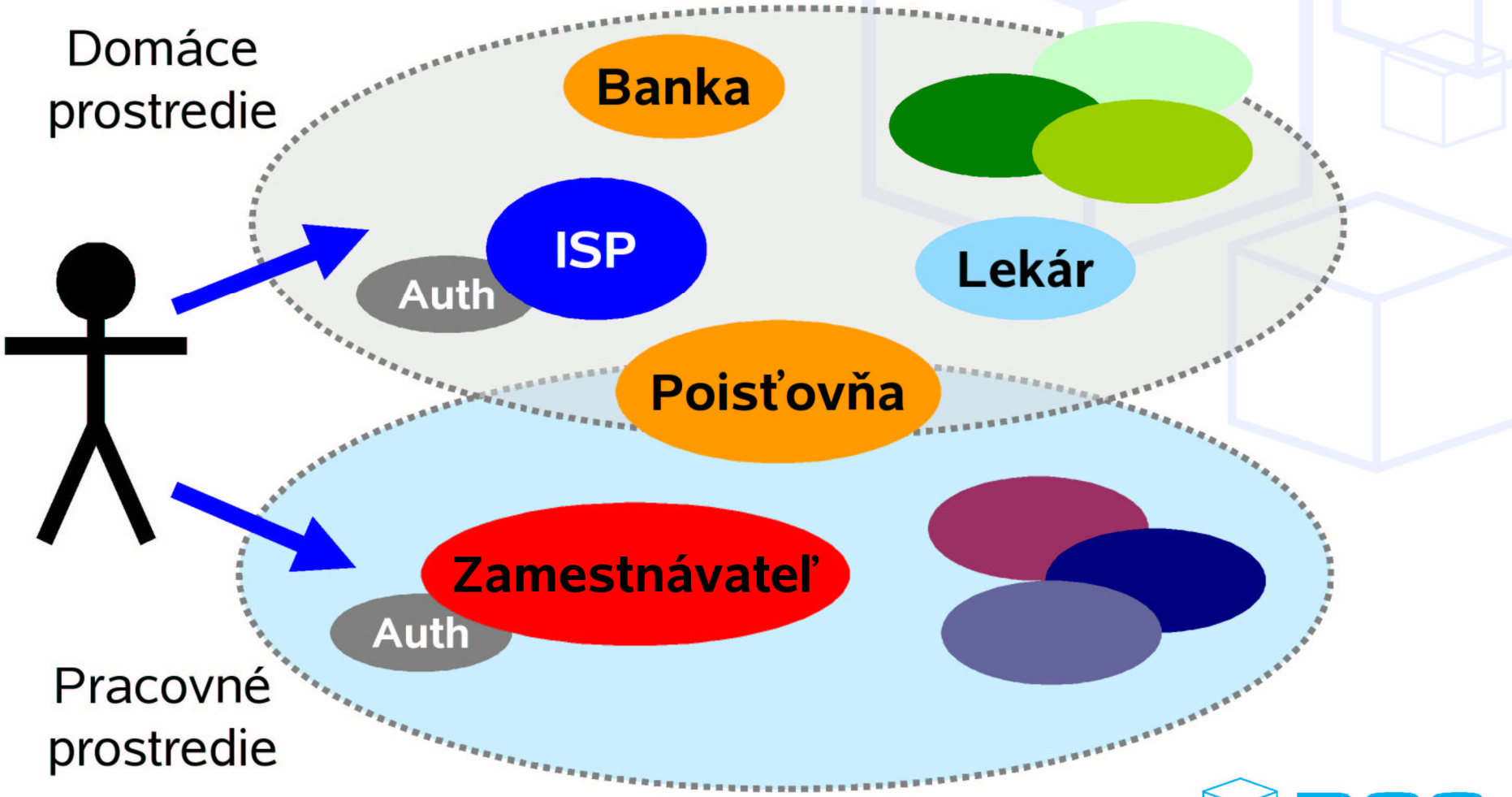
BGS
Business Global Systems

Privacy, User in control



BGS
Business Global Systems

Circle of trust



BGS
Business Global Systems

Digital Identity technológie

- Base: eXtensible Markup Language (XML)
- **Security Association Markup Language** (SAML)
- XML Key Management Specification (XKMS)
- Platform for Privacy Preferences (P3P)
- **Web services security specification** (WS-Security)
  - Microsoft, IBM, Verisign, Sun Microsystems
- **Liberty Alliance Project**
  - Sun Microsystems, HP, SONY, RSA Security, NOKIA, …
- Microsoft TrustBridge & Palladium Projects

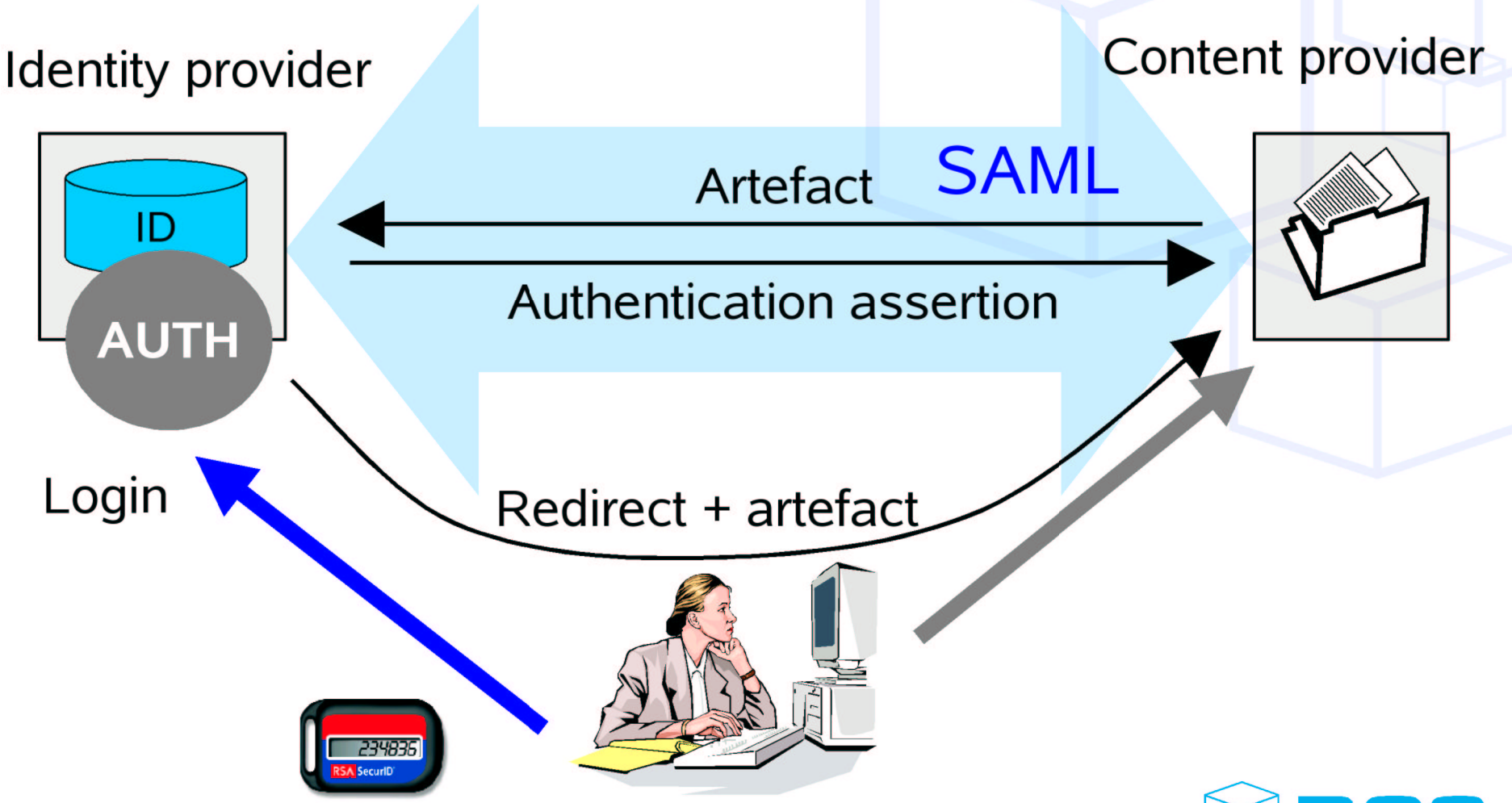
BGS
Business Global Systems

Security Association Markup Language (SAML)

- Transport of ‘assertions’ across systems
  - Authentication assertion
  - Attribute assertion
  - Authorization assertion
- Origin: OASIS
- Uses XMLdsig and SSL/TLS

BGS
Business Global Systems

SAML Browser/artefact



BGS
Business Global Systems

Authentication assertion

Dolupodpísaný IdentityProvider1 týmto potvrdzuje, že používateľ „D3ADB33F“ sa úspešne prihlásil dňa 04/02/2002 00:42:00 za použitia „silnej“ autentifikácie.

V charon.bgs.sk dňa 04/02/2002 01:10:15,

IdentityProvider1, v.r.

(samozrejme zapísané v XML)

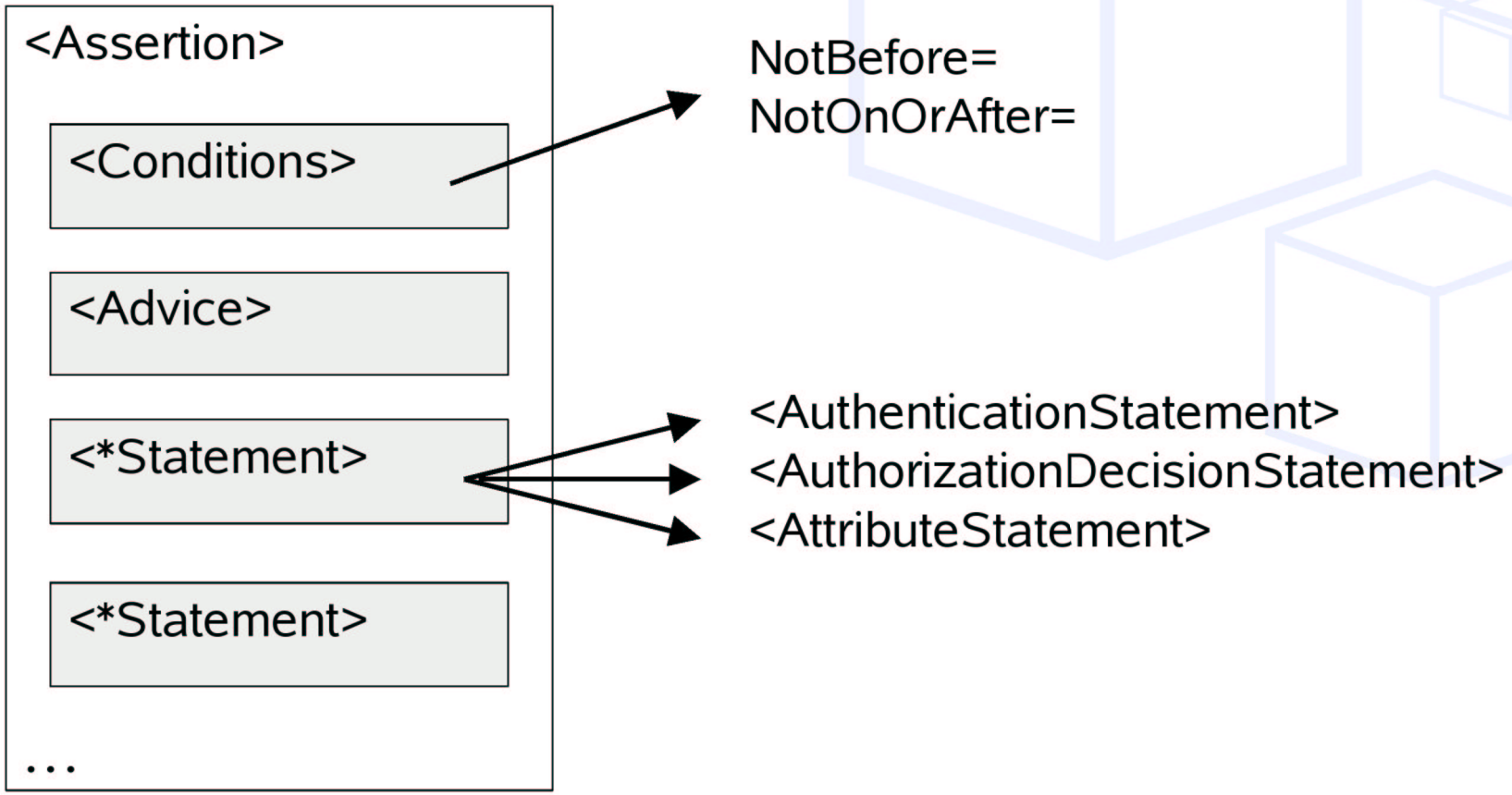
BGS
Business Global Systems

Authentication Statement

```
<saml:assertion Issuer="idprovider1.com"…>

    <saml:Conditions NotBefore=… NotAfter=…/>

    <saml:AuthenticationStatement
      AuthenticationMethod="strong"
      AuthenticationInstant="04/02/2002 00:42:00" >
      <saml:subject …>D3ADB33F</saml:subject>
    </saml:AuthenticationStatement>

 </saml:Assertion>
```

BGS
Business Global Systems

SAML document structure



BGS
Business Global Systems

Agenda

- Čo?
- Prečo?
- Ako?
- A čo teraz?
- A vôbec ...

BGS
Business Global Systems

Záver

- Digital identity
  - Bezpečnostná infraštruktúra
  - Súkromie, bezpečnosť, pohodlie
  - Väčšie možnosti

BGS
Business Global Systems

What do you want to know today?

BGS
Business Global Systems

Ďakujem za pozornosť

Ing. Radovan Semančík
Business Global Systems
semancik@bgs.sk

BGS
Business Global Systems