Internet Security

Ing. Radovan Semančík

6. Linux weekend, Marec 2002, Bratislava

Agenda

- Úvod
- Access control
- Kryptografické protokoly
- VPN
- Záver

Bezpečnosť

BGS
Business Global Systems

Úvod

Security - čo to vlastne je?

~~“Nehackniteľnosť”~~	Risk management
~~Akcia~~	Process
~~Len systémy~~	Aj ľudia, prostredie, ...

BGS
Business Global Systems

Security goals

Ciele:

Confidentiality

Integrity

Availability

Metódy:

Access control

Organizational procedures

Cryptography

Physical security devices

Biometrics

….

BGS
Business Global Systems

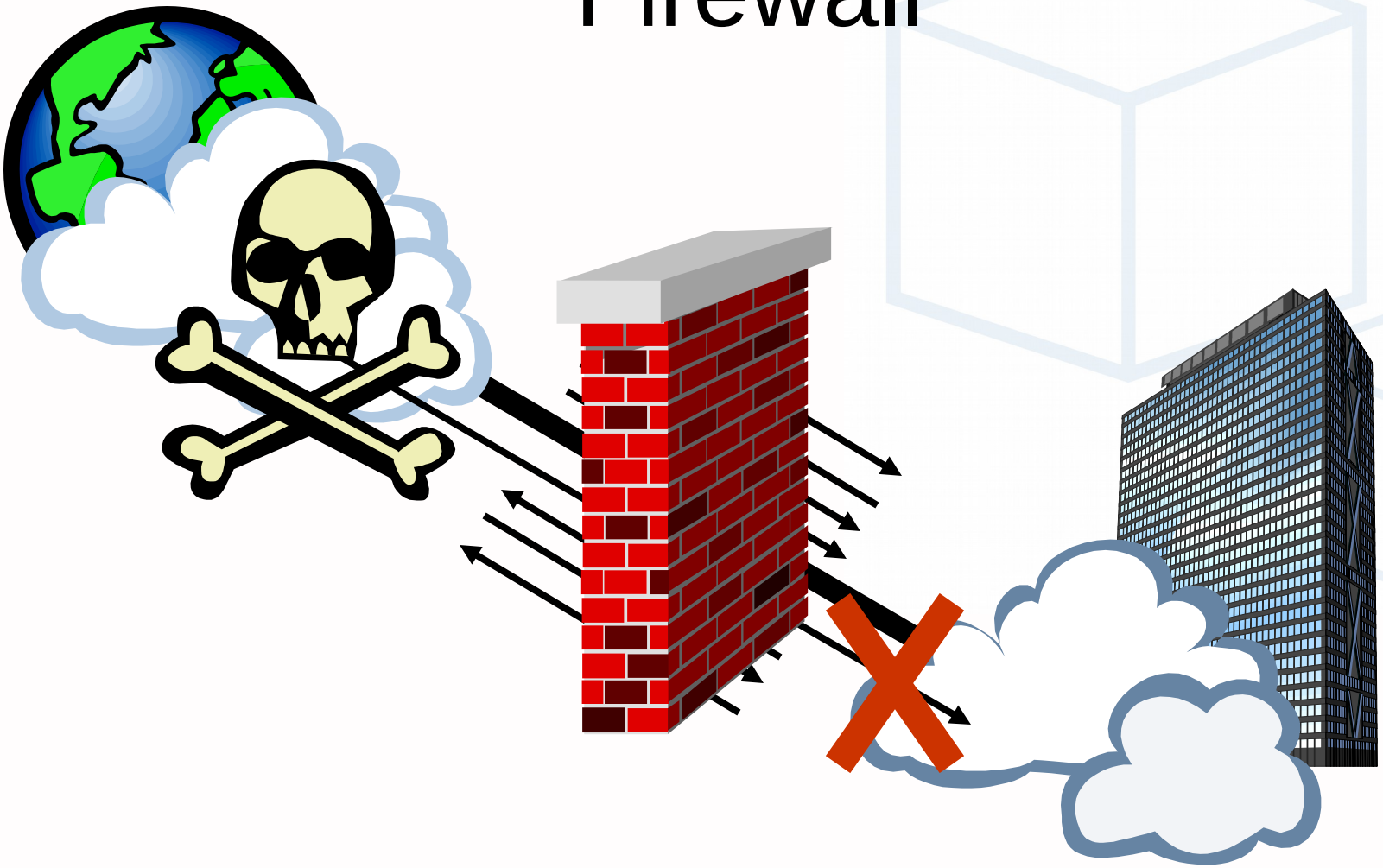
Agenda

- Úvod
- Access control
  - Authorizácia
  - Firewall
  - DMZ
- Kryptografické protokoly
- VPN
- Záver

Access control

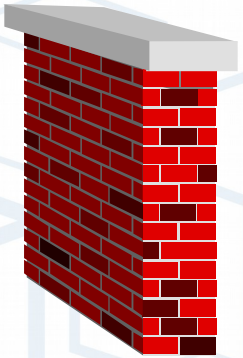
- Autorizácia
  - Rozhodnutie kto má kam prístup
  - porovnaj: Autentifikácia - určovanie identity
- Na rôznych úrovniach
  - Komunikačná sieť
  - Operačný systém
  - Aplikácia

Firewall



Business Global Systems

Firewall



TCP S=10.5.5.5 D=10.2.2.2 P=25

TCP S=212.15.18 D=10.2.2.2 P=23

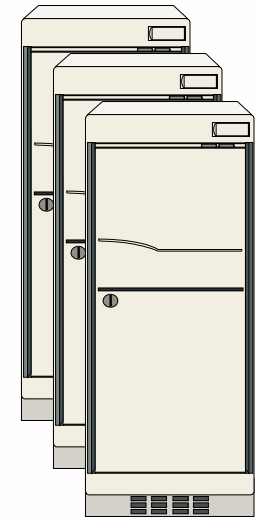
10.5.5.5 → 10.2.2.2:25	ALLOW
10.2.2.* → *:80	ALLOW
* → *	DENY

BGS
Business Global Systems

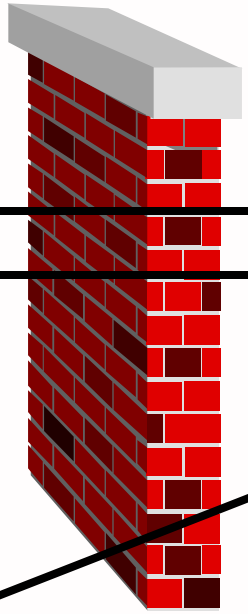
Druhy firewallov

- Bezstavový paketový filter
  - **+** Rýchle, lacné
  - **-** Zložité pravidlá, málo bezpečné
- Stavový firewall
  - **+** Vyšia bezpečnosť, ľahšia konfigurácia
  - **-** Drahé, náročné
- Aplikačné proxy
  - Závislé od aplikácie

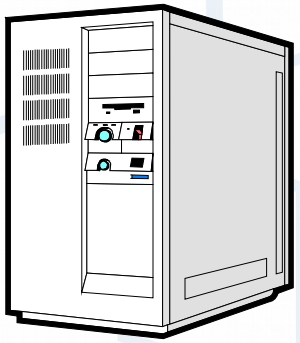
Bezstavový paketový filter



DNS server
10.10.10.10



DNS
port 53
(UDP)



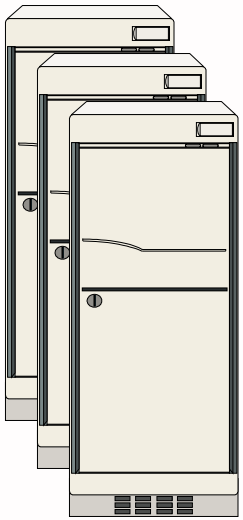
10.1.1.10

#$%!@
port 53
(UDP)

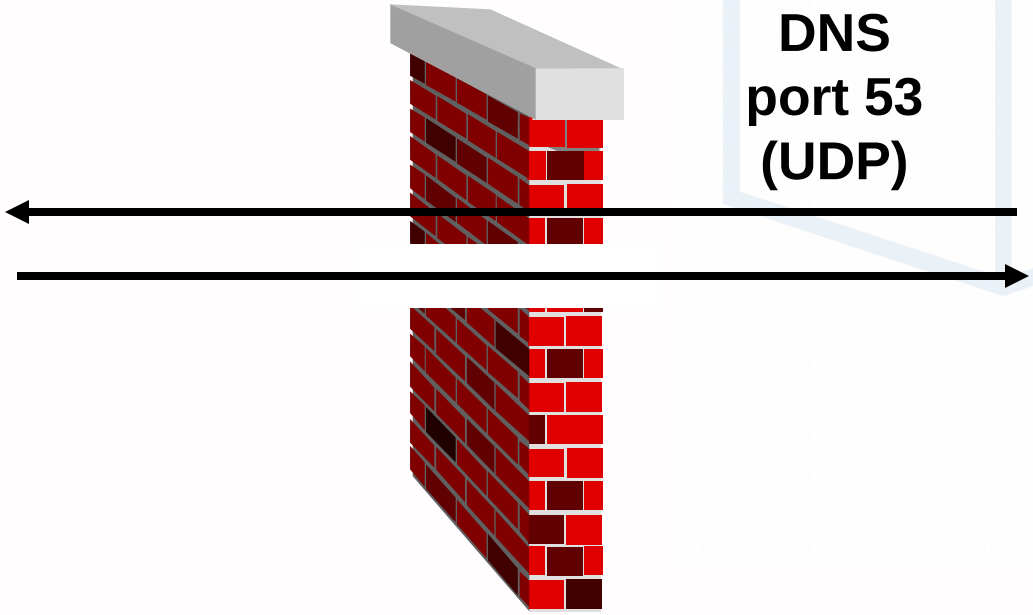
UDP port 53 → *	ALLOW
* port 53 → 10.1.1.10	ALLOW
* → *	DENY

BGS
Business Global Systems

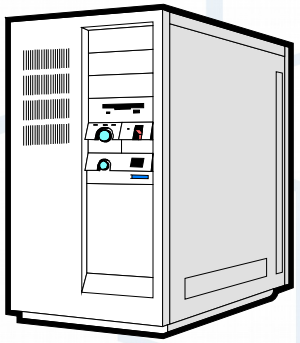
Stavový firewall



DNS server
10.10.10.10



DNS
port 53
(UDP)

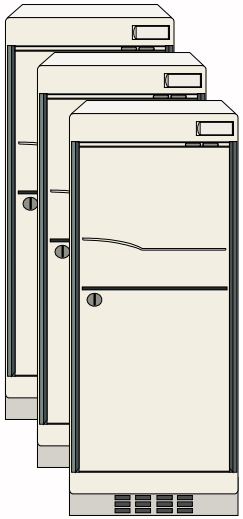


10.1.1.10

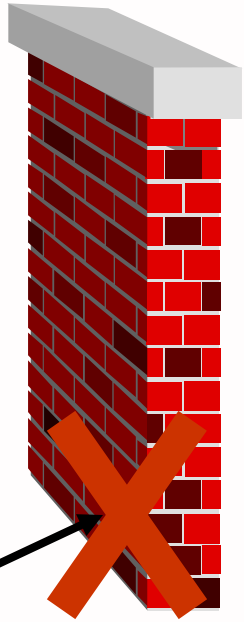
UDP port 53 → *	ALLOW
* port 53 reply→ 10.1.1.10	ALLOW
* → *	DENY

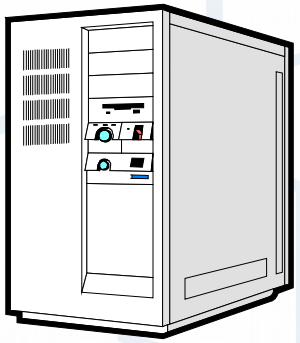
BGS
Business Global Systems

Stavový firewall



DNS server
10.10.10.10





10.1.1.10

#$%!@
port 53
(UDP)

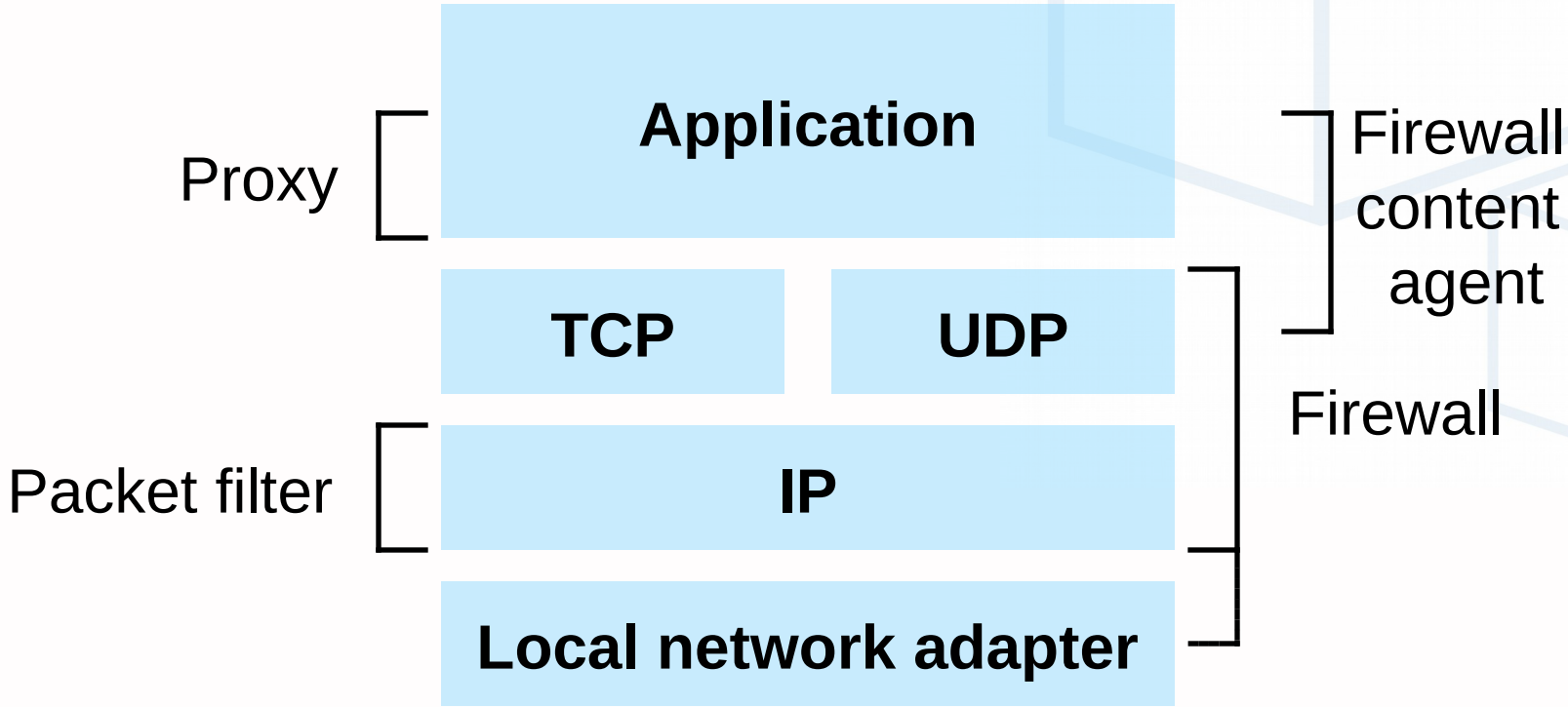
UDP port 53 → *	ALLOW
* port 53 reply→ 10.1.1.10	ALLOW
* → *	DENY

BGS
Business Global Systems

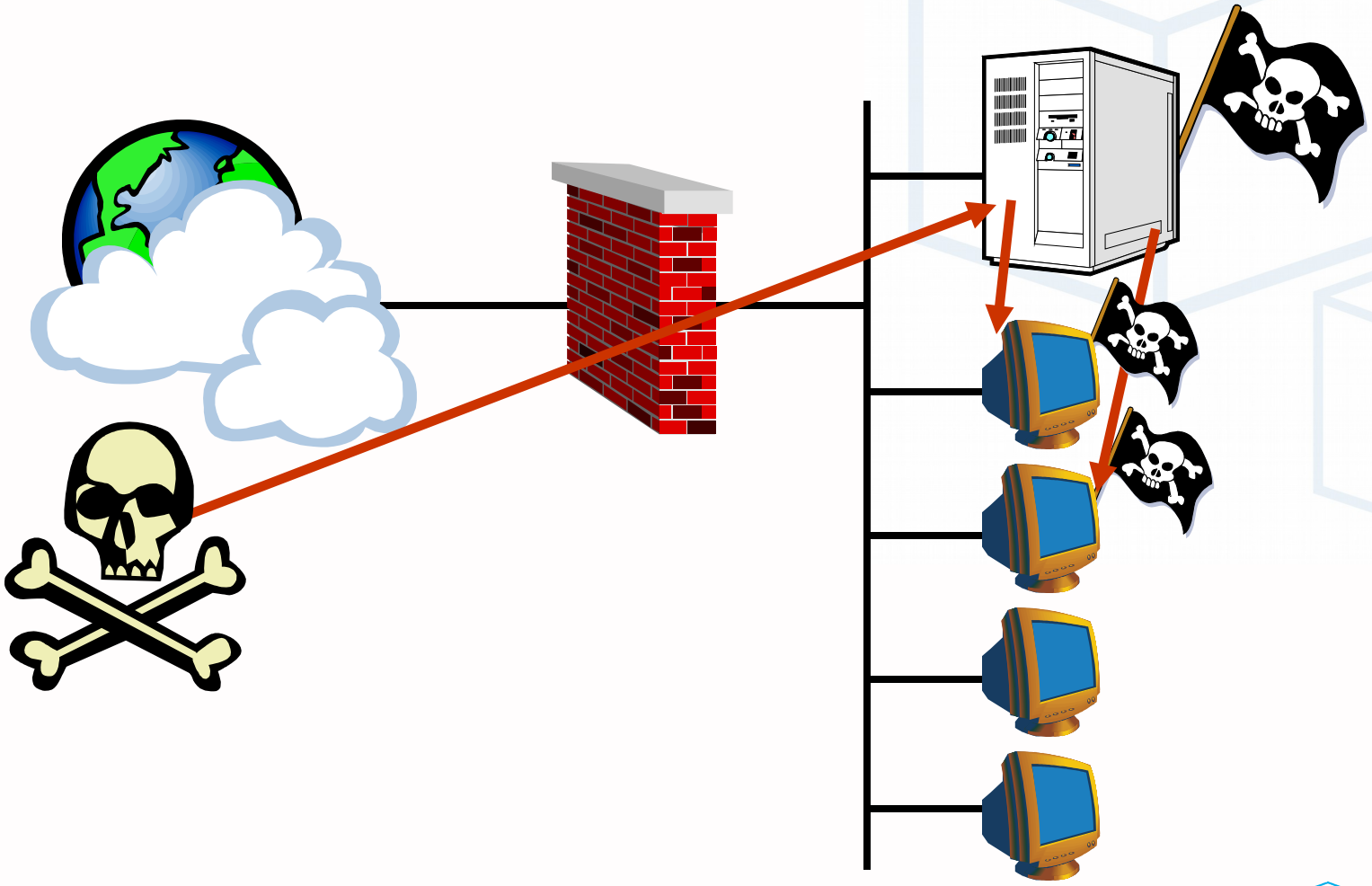
Stavový firewall

- TCP spojenia
  - tabuľka aktívnych spojení
- DNS, FTP, H.323 a spol.
  - Závislé pravidlá
- Aplikačný agenti (content agents)
  - Antivírová ochrana, URL blocking, ...

Firewalling a TCP/IP



Nasadenie firewallu

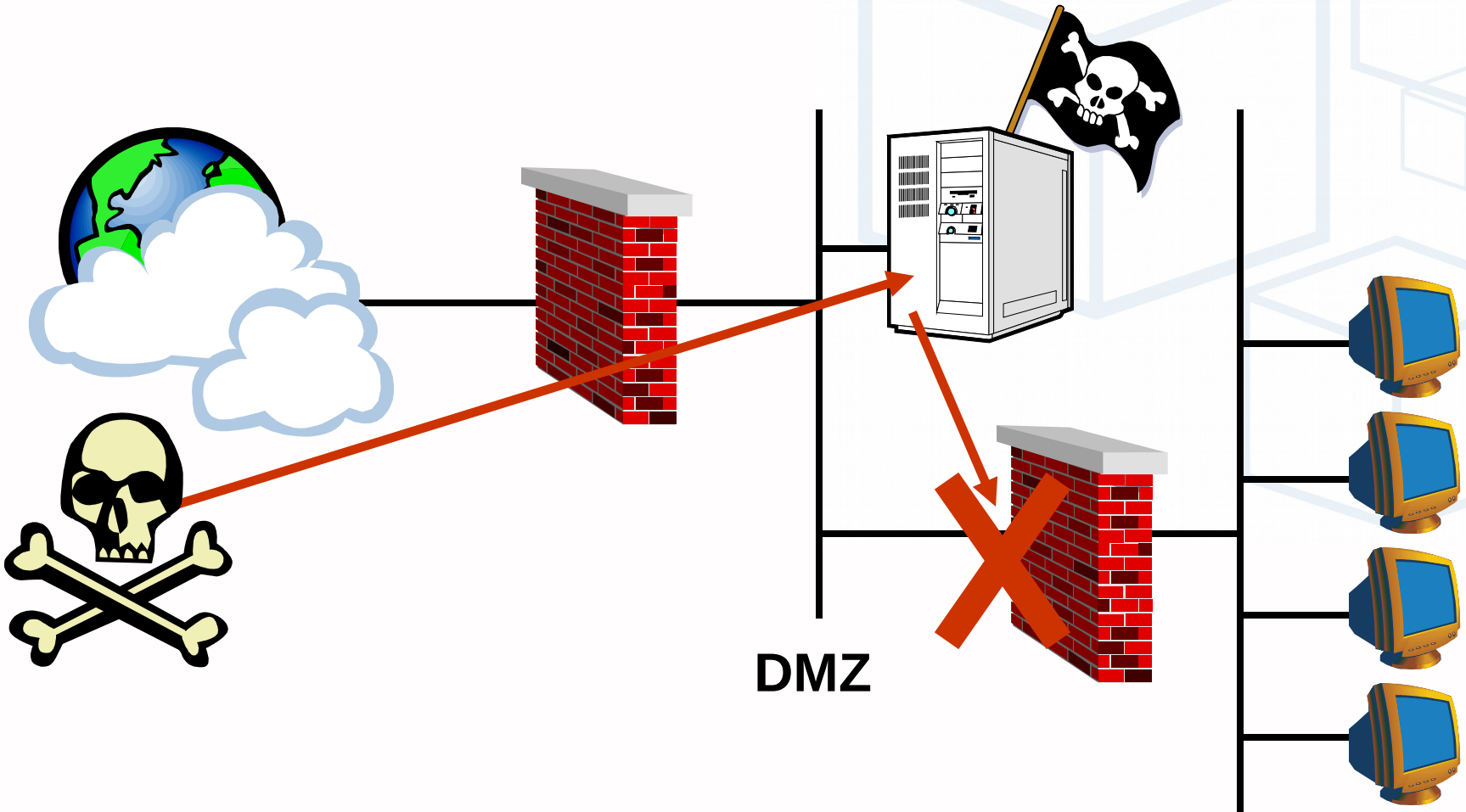


Business Global Systems

DMZ

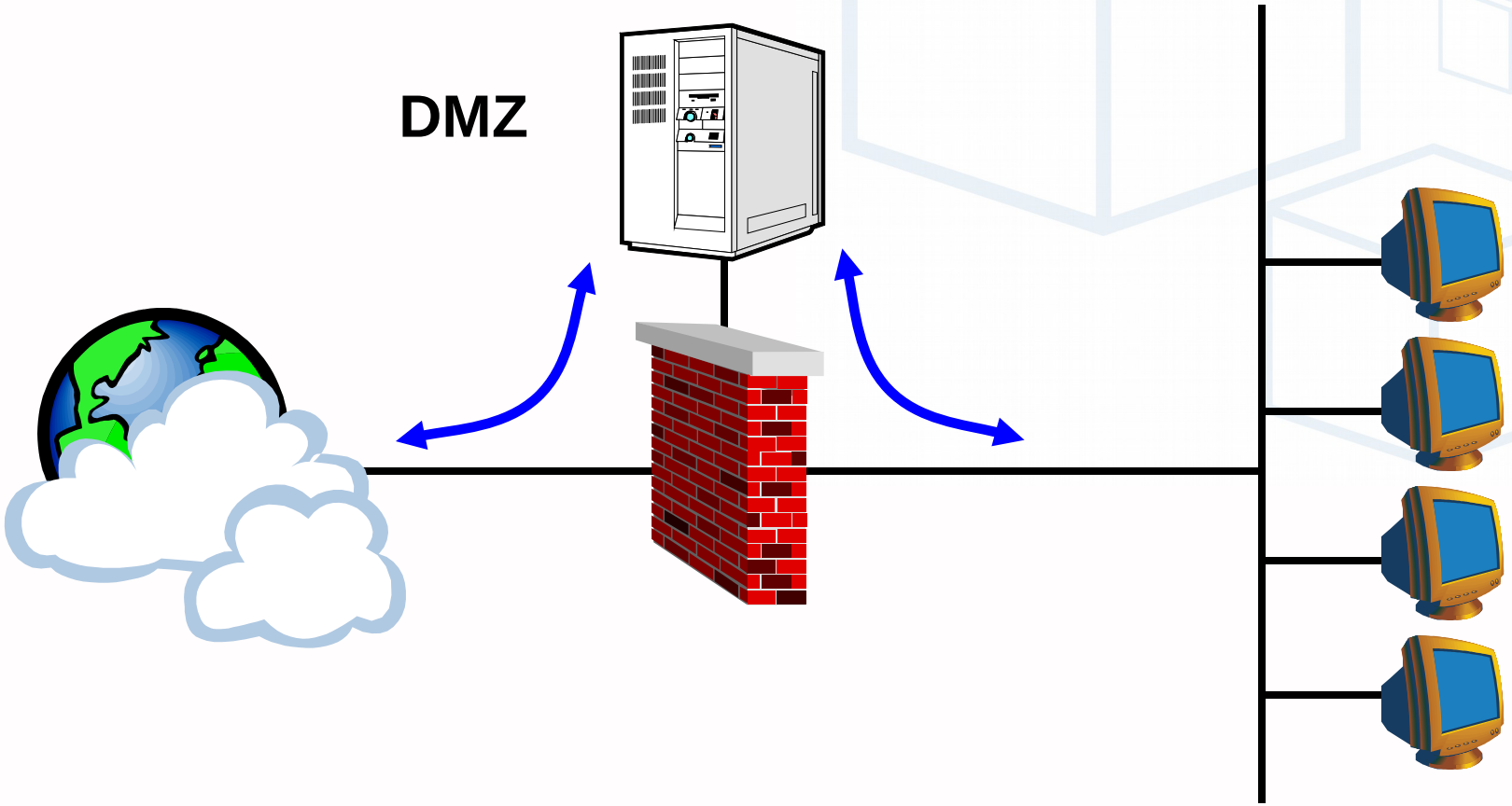
BGS
Business Global Systems

Demilitarized zone (DMZ)



BGS
Business Global Systems

DMZ - úsporná verzia



BGS
Business Global Systems

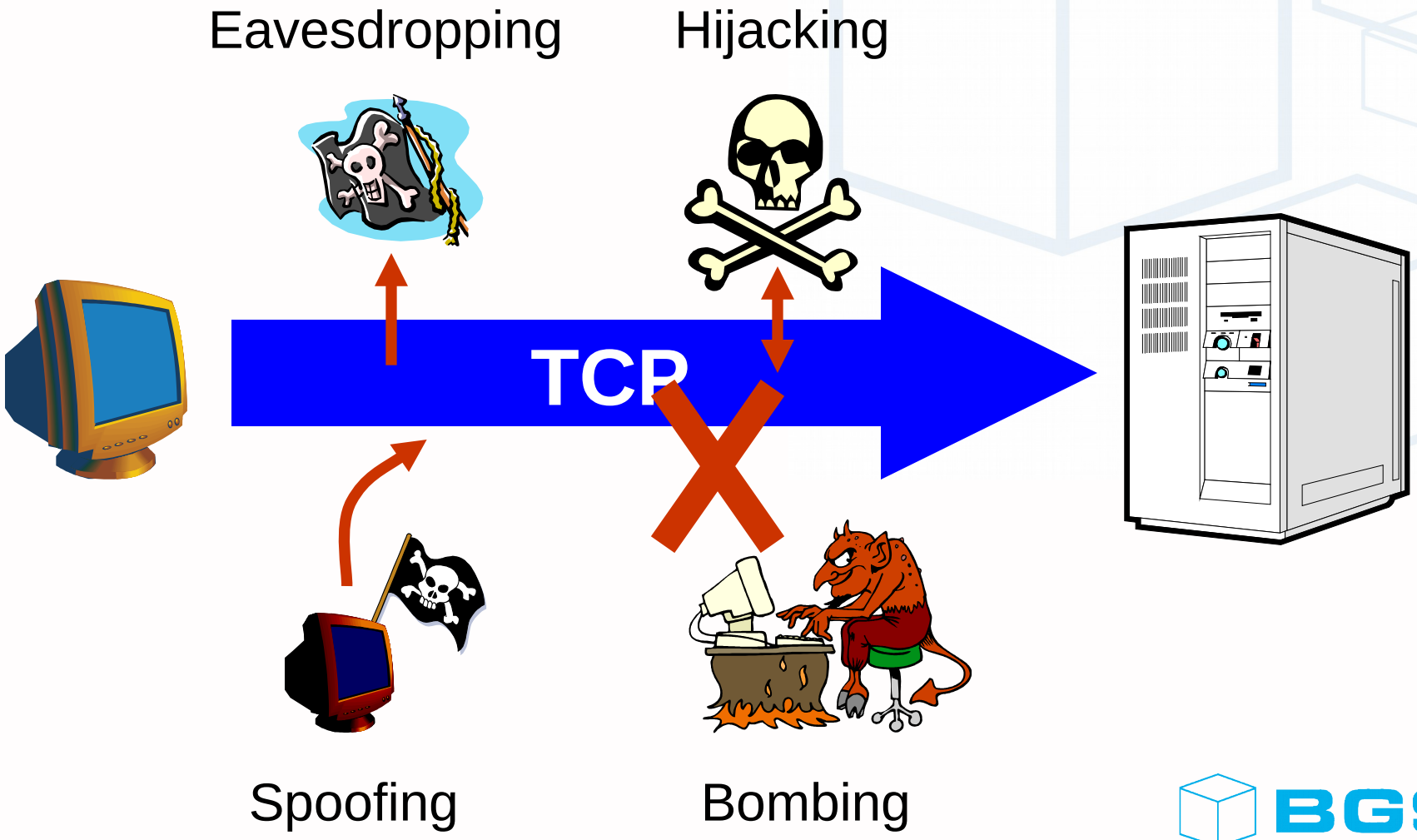
Agenda

- Úvod
- Access control
- Kryptografické protokoly
  - SSH, PGP
  - X.509
  - SSL, TLS, S/MIME
- VPN
- Záver

Na počiatku bola tma

telnet

Telnet insecurity



BGS
Business Global Systems

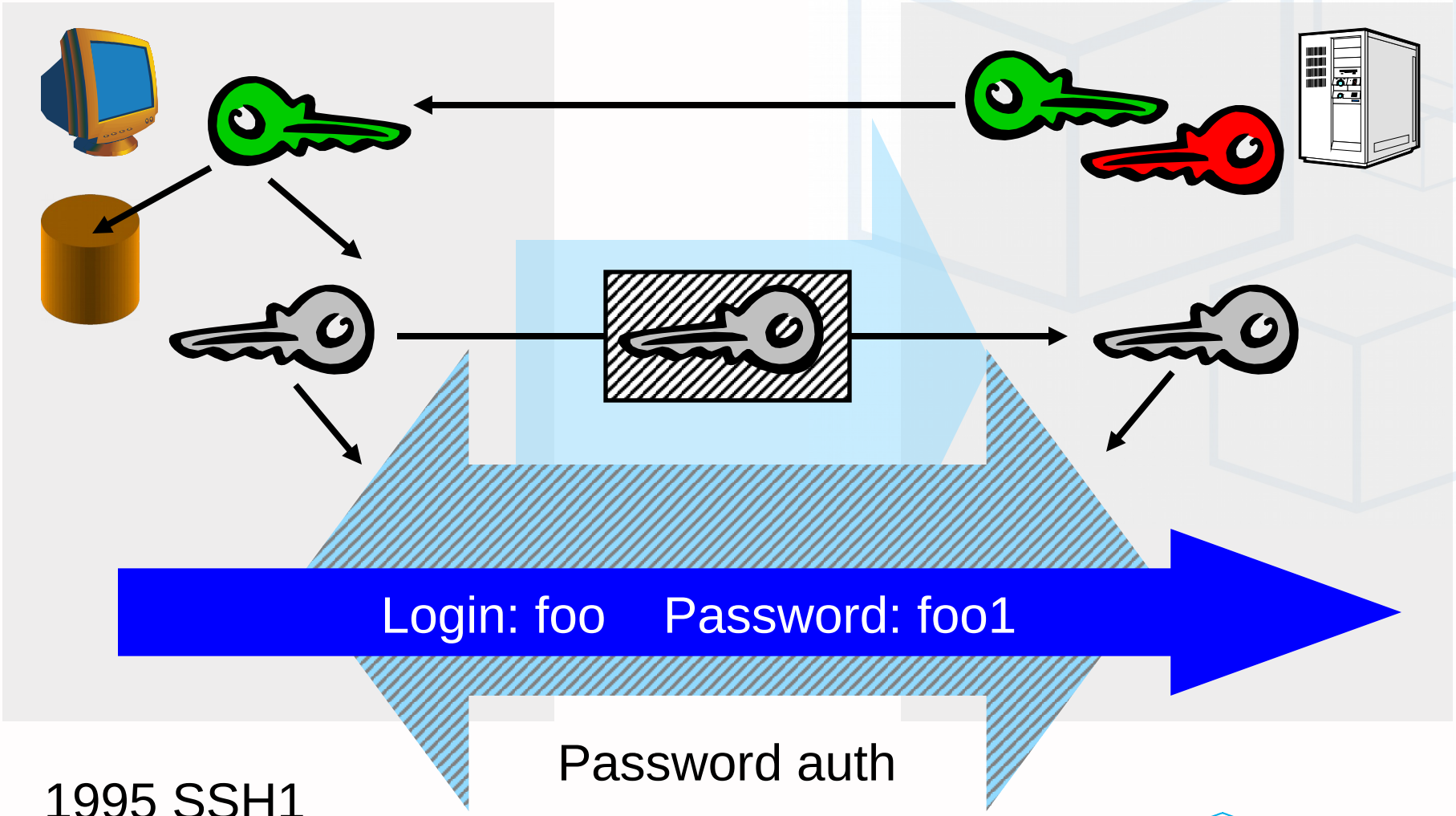
“Strong” authentication

- S/Key, SecureID, ...
  - Kryptografické technológie autentifikácie
  - TCP kanál zostáva nezašifrovaný
  - Možný hijacking, odpočúvanie, …
  - V čase ITAR* použiteľné, teraz problém
  - Použiteľné ako “zlepšená” autentifikácia

* International Trade in Arms Regulation

BGS
Business Global Systems

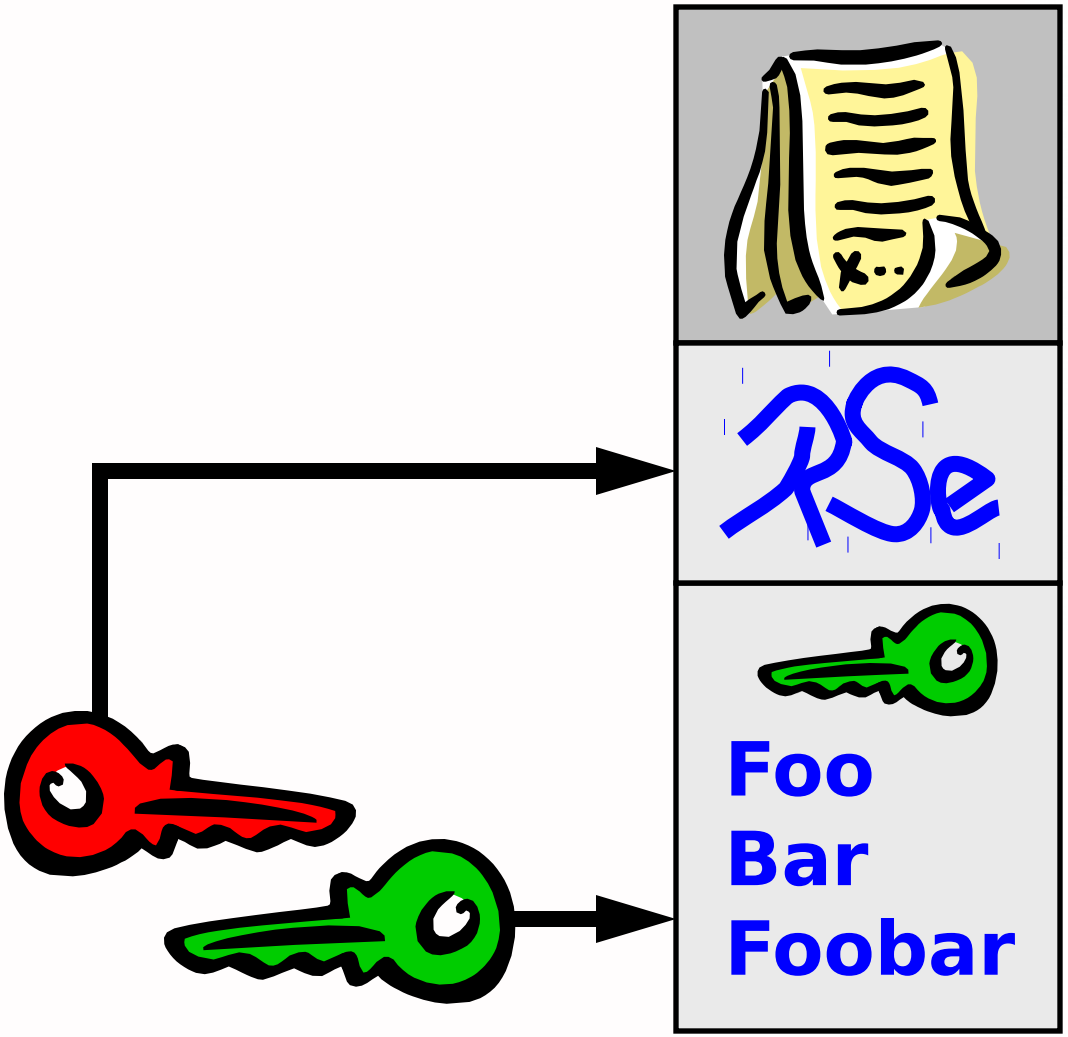
SSH - Secure shell



1995 SSH1
1997 SSH2 (IETF)

BGS
Business Global Systems

Pretty Good Privacy - PGP



Philip R. Zimmermann
1991: v1.0
1995: v2.62i
1997: v5.0 (5.0i)
1999: GnuPG 1.0

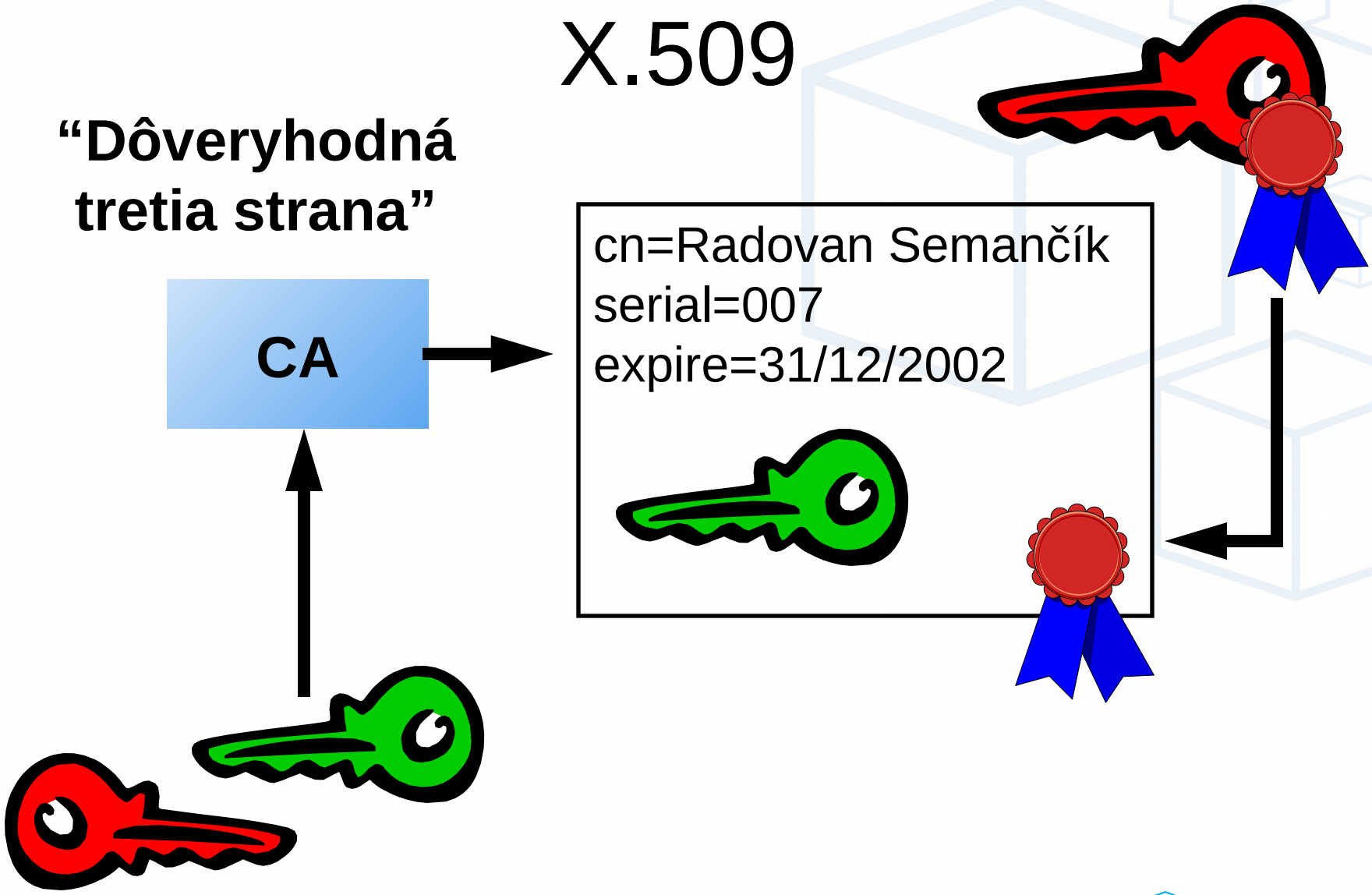
BGS
Business Global Systems

PGP & SSH problems

- Keys, keys, keys
  - SSH: uložené na lokálnom disku
  - PGP: Web of trust
- Štruktúra
  - SSH: žiadna, flat files
  - PGP: Web of trust, chaotická
- Vhodné pre malé systémy a nekomerčný Internet

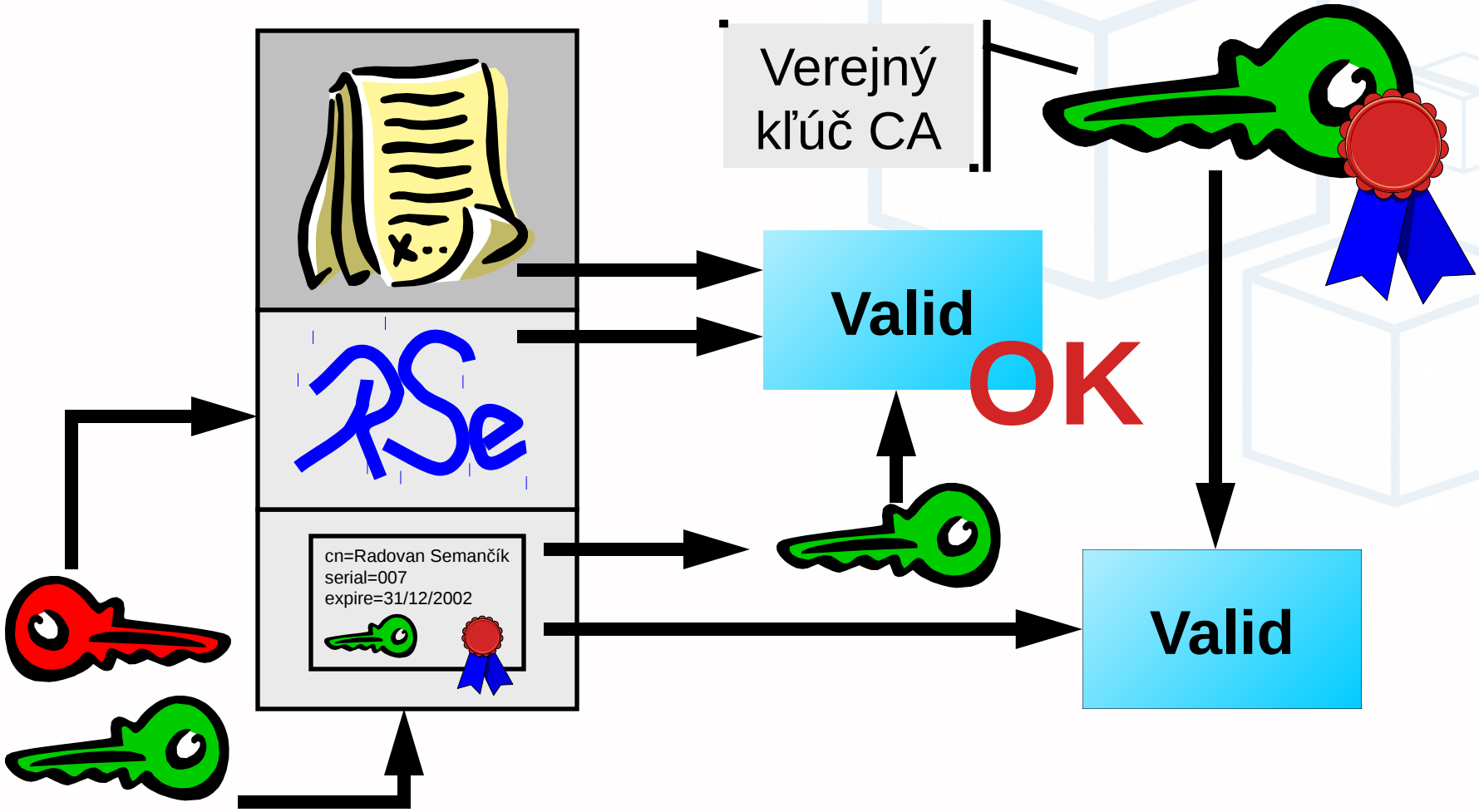
X.509

“Dôveryhodná tretia strana”



BGS
Business Global Systems

Overovanie certifikátu



Business Global Systems

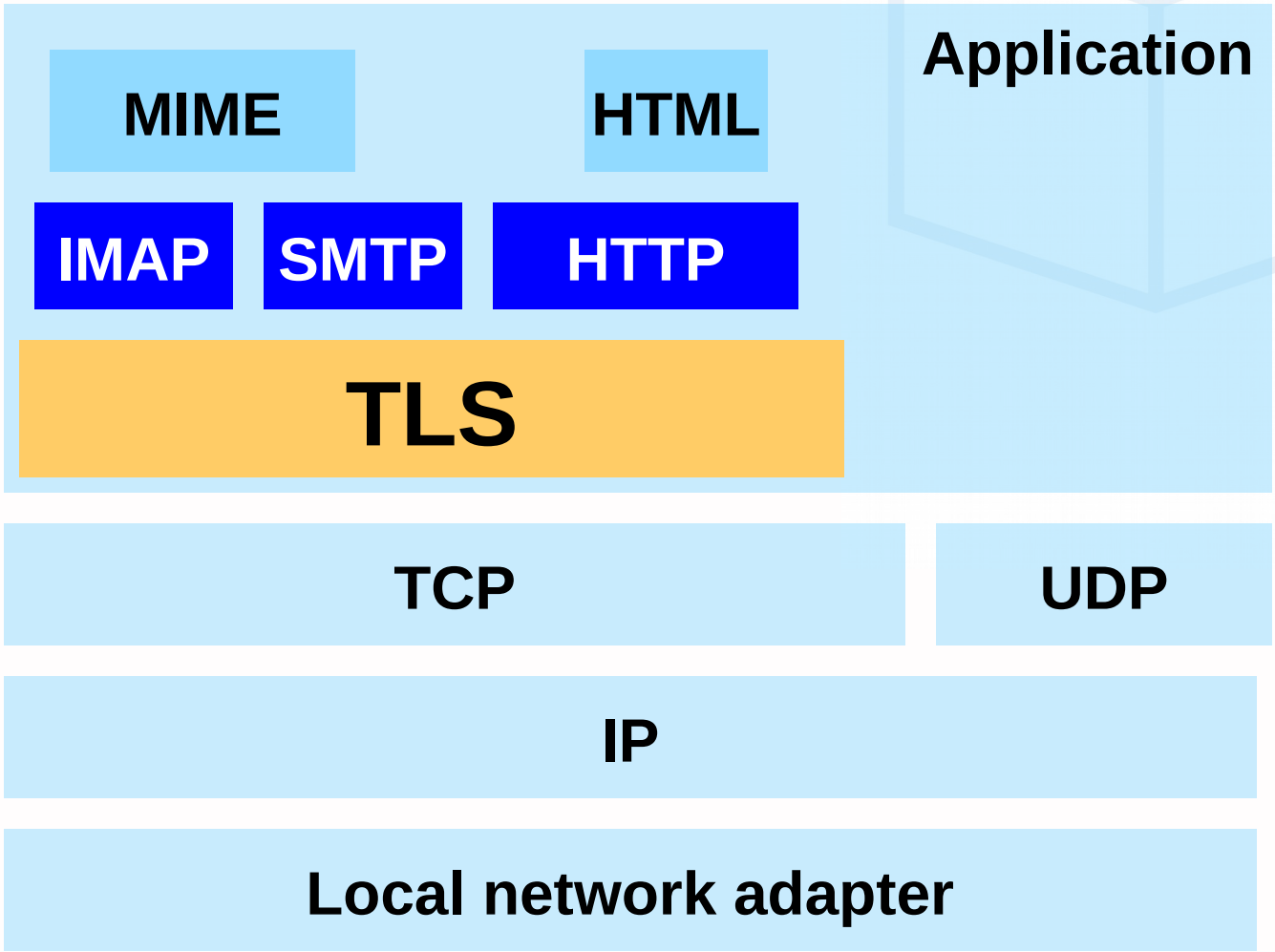
HTTPS

BGS
Business Global Systems

Transport Layer Security

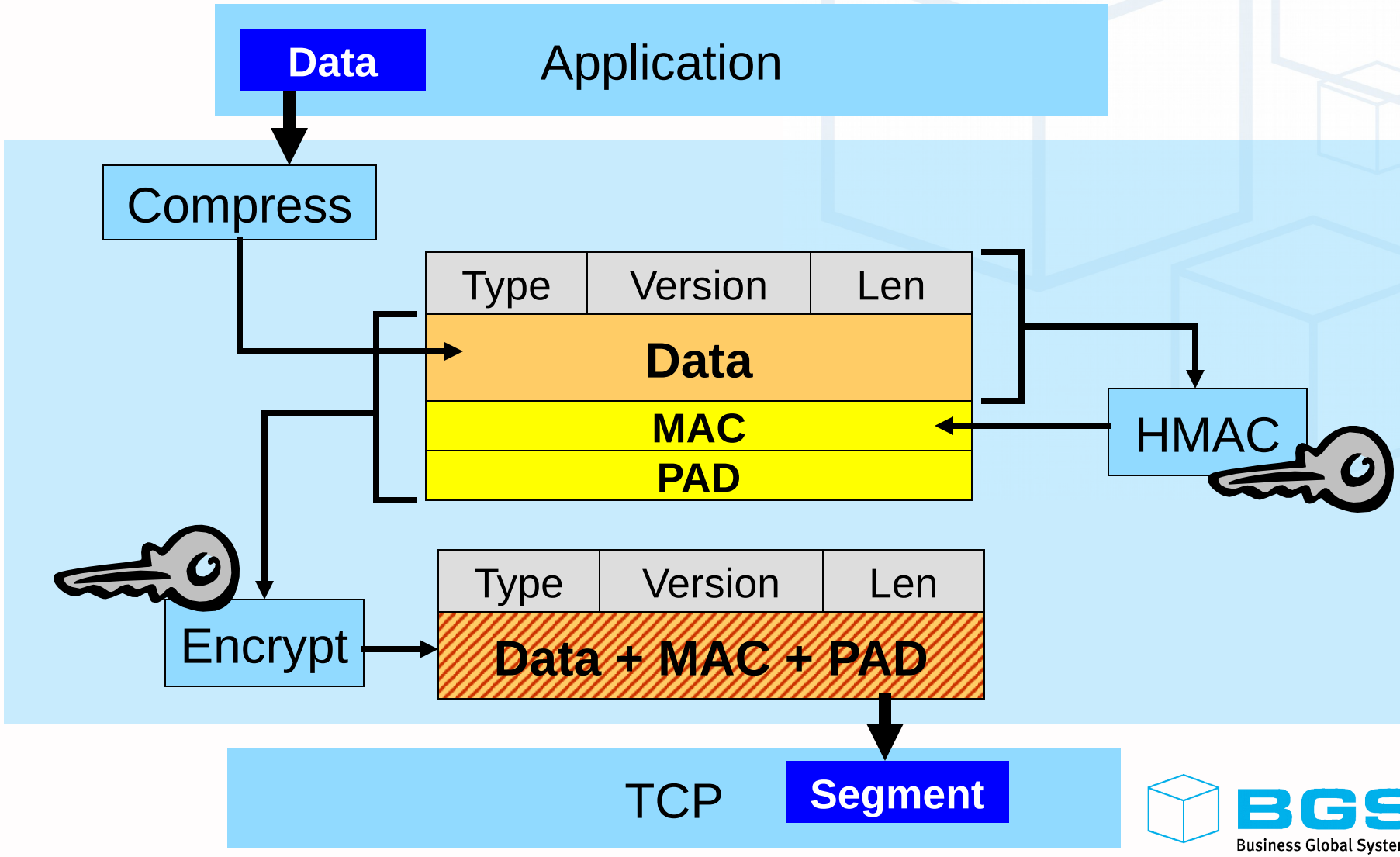
- Pôvodne SSL - Secure Socket Layer
- 1994: Netscape SSL 1.0 (nenasadený)
- 1994: Netscape SSL 2.0
- 1996: Netscape SSL 3.0
  - Rieši problémové miesta SSL 2.0
- 1999: TLS 1.0 (RFC 2246)
- súčasnosť: RFC 2246bis (IETF)

TLS & TCP/IP



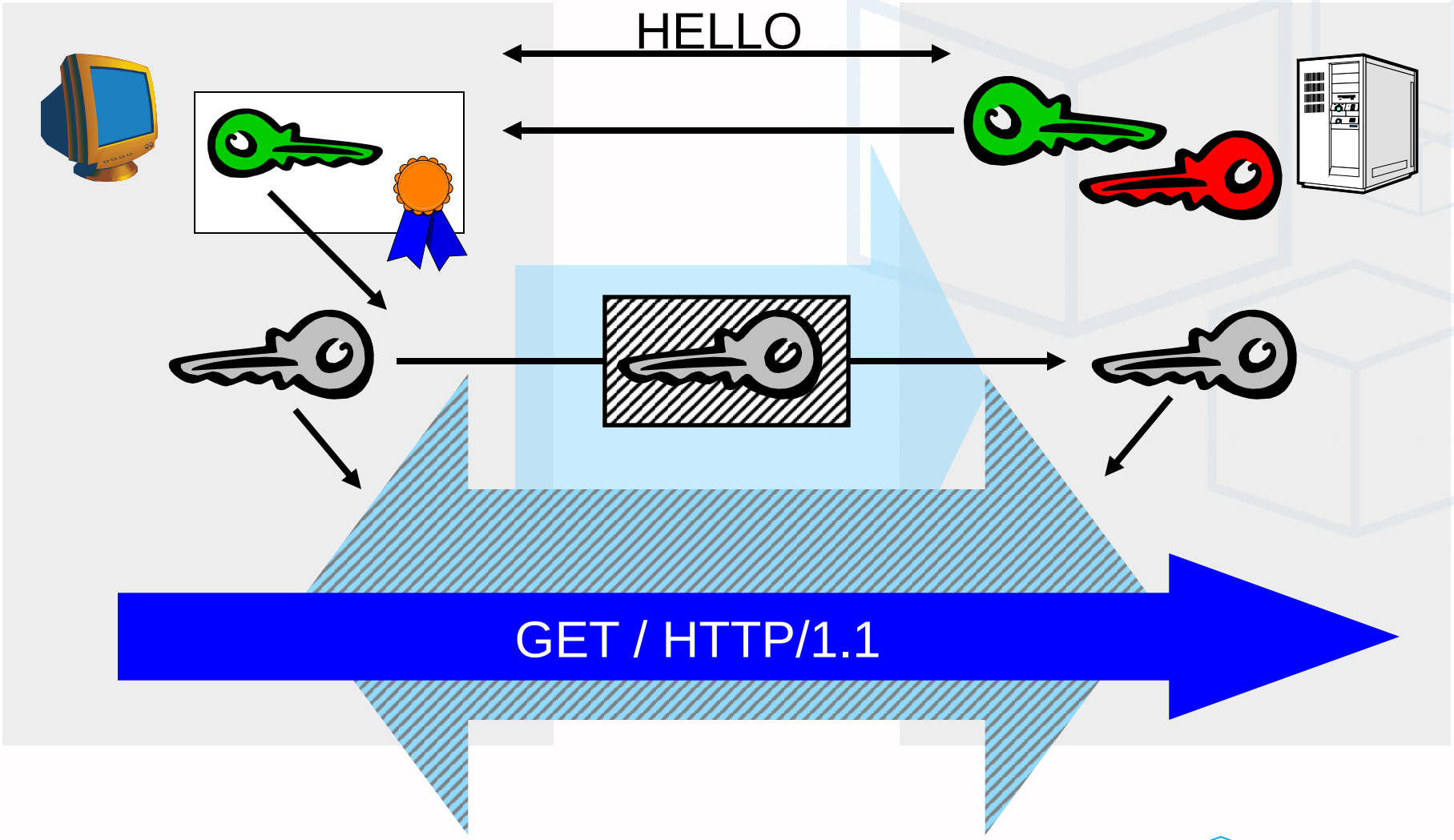
BGS
Business Global Systems

TLS record layer



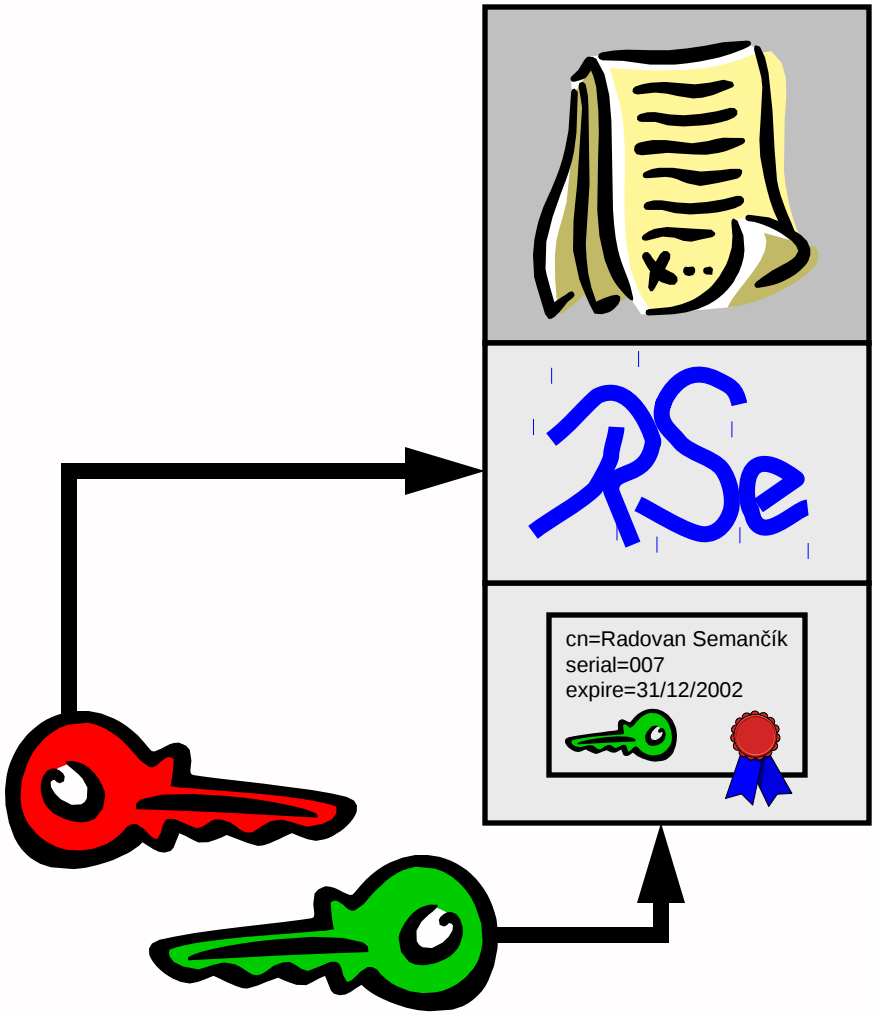
Business Global Systems

TLS handshake



BGS
Business Global Systems

S/MIME

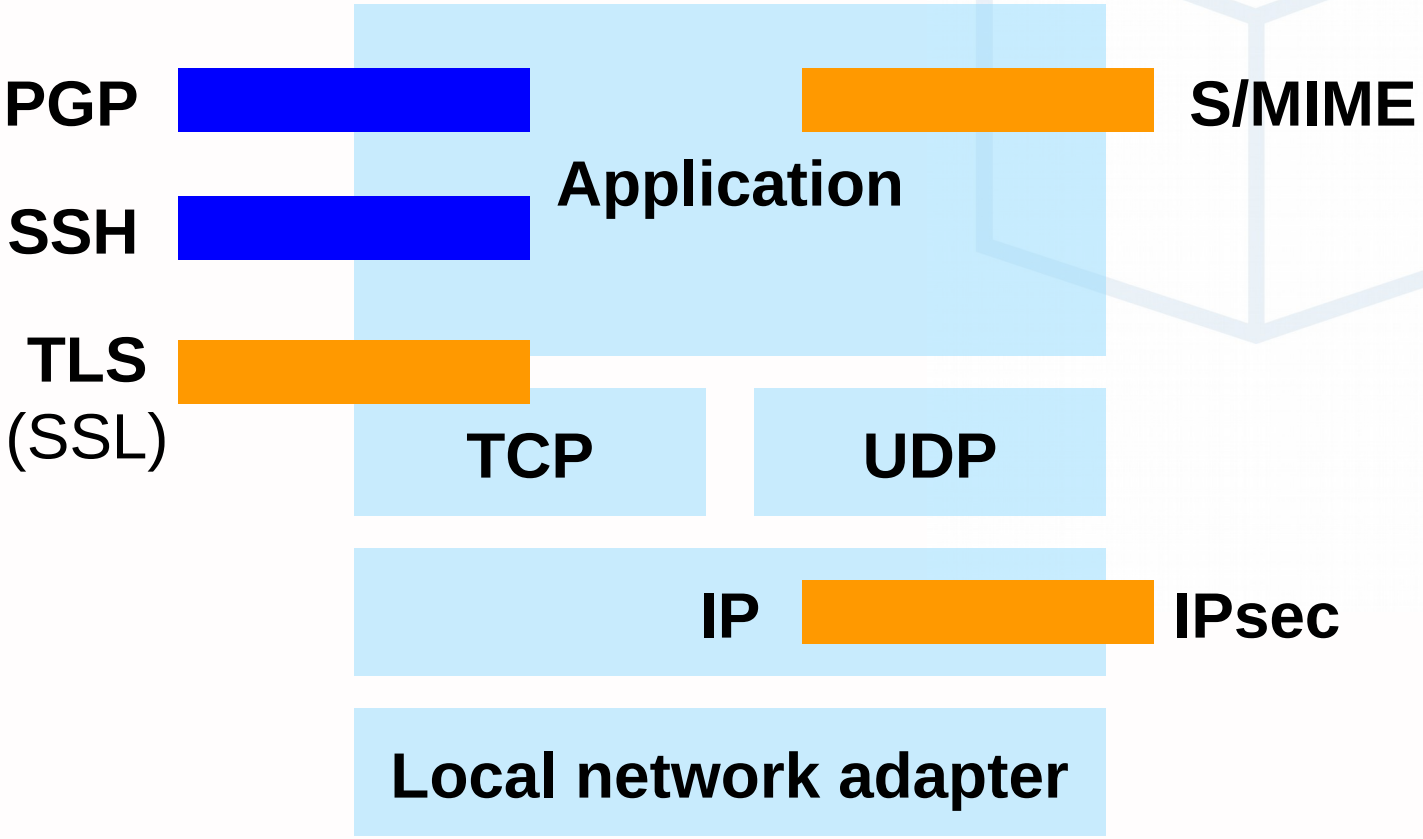


Nadstavba MIME

1995: RSA labs
1998: S/MIME v2 RFC 2311
1999: S/MIME v3 RFC 2633

BGS
Business Global Systems

TCP/IP security options



BGS
Business Global Systems

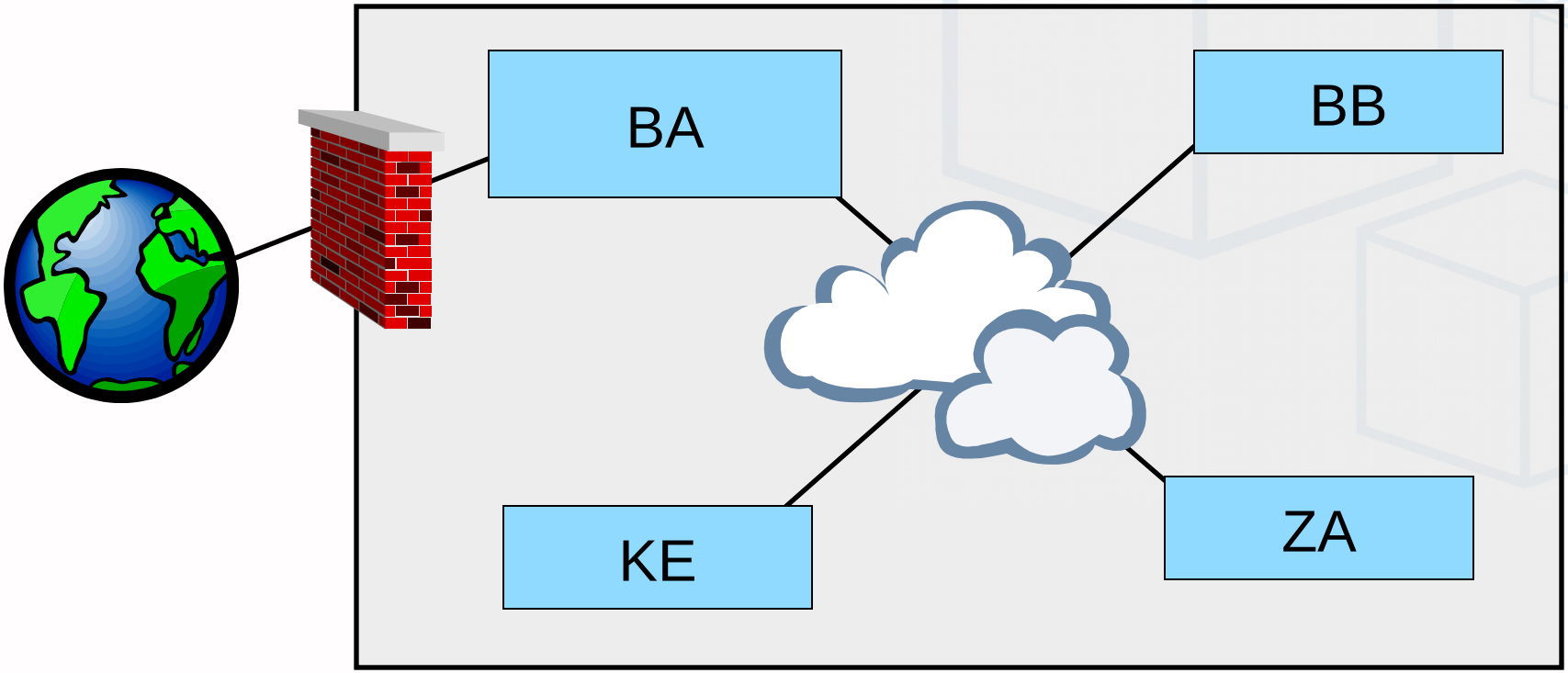
Prečo X.509?

- PGP, SSH, etc.
  - Prorietary key managemet
  - Infrastructure? Policy?
- TLS, IPsec, S/MIME, etc.
  - X.509 infrastructure, key management
  - CA controls the key policies
  - Key recovery (not only “escrow”)

Agenda

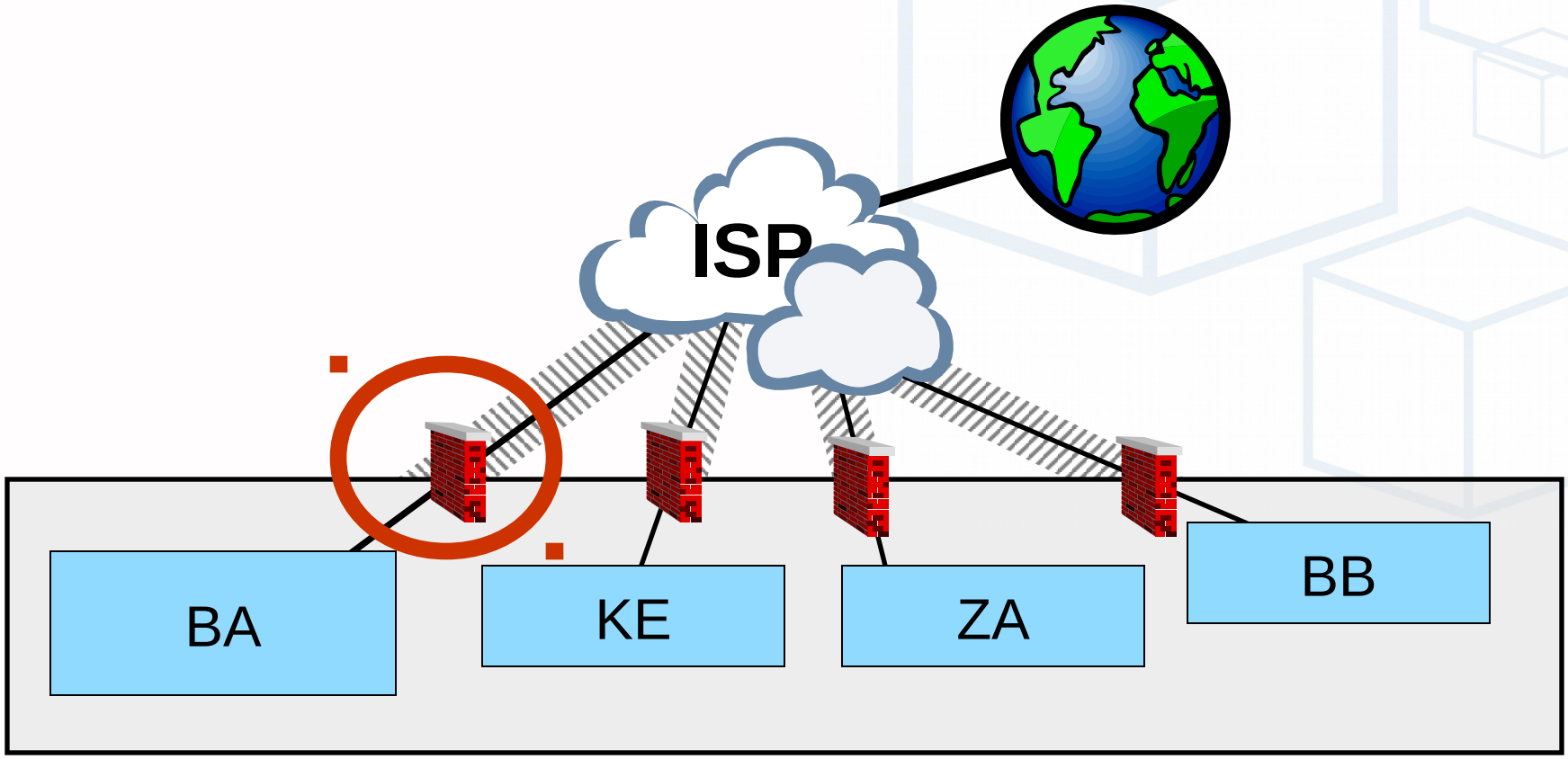
- Úvod
- Access control
- Kryptografické protokoly
- VPN
  - VPN koncept
  - IPsec
  - IKE
- Záver

Private Network



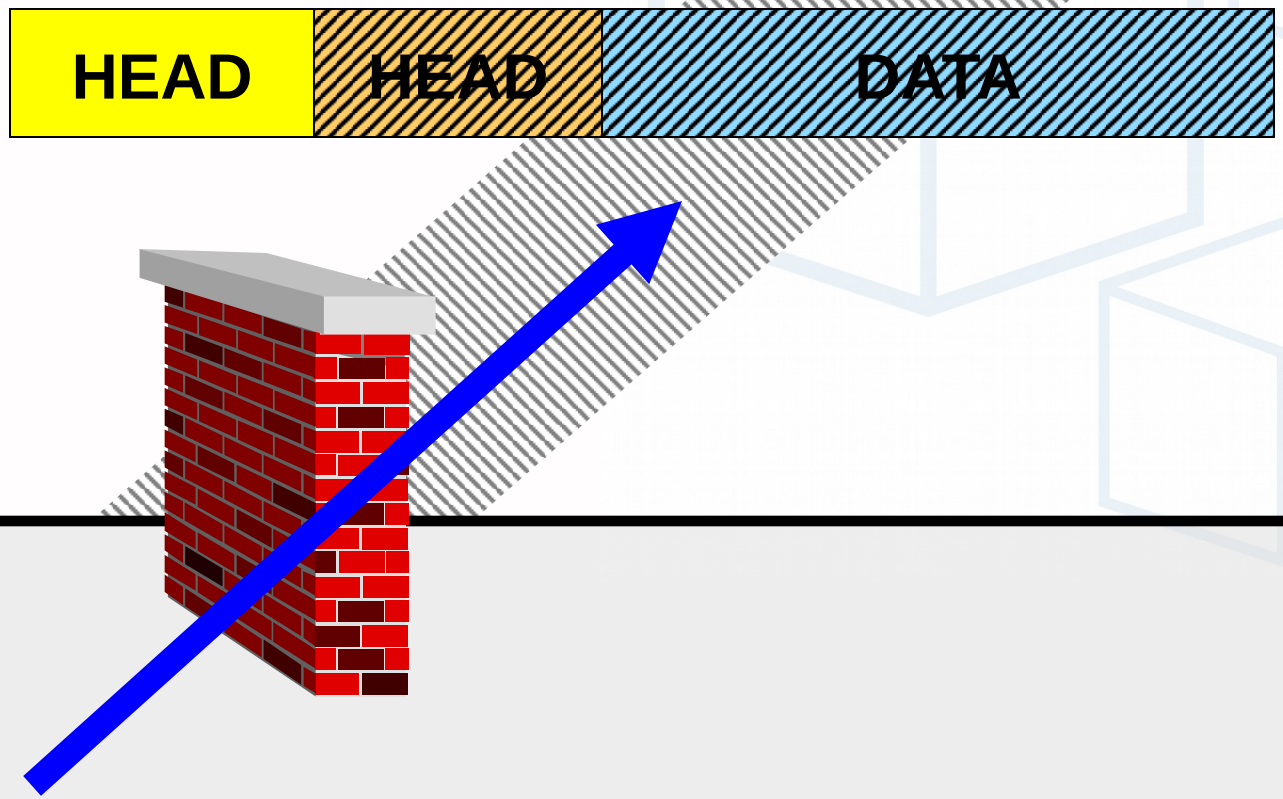
BGS
Business Global Systems

Virtual Private Network

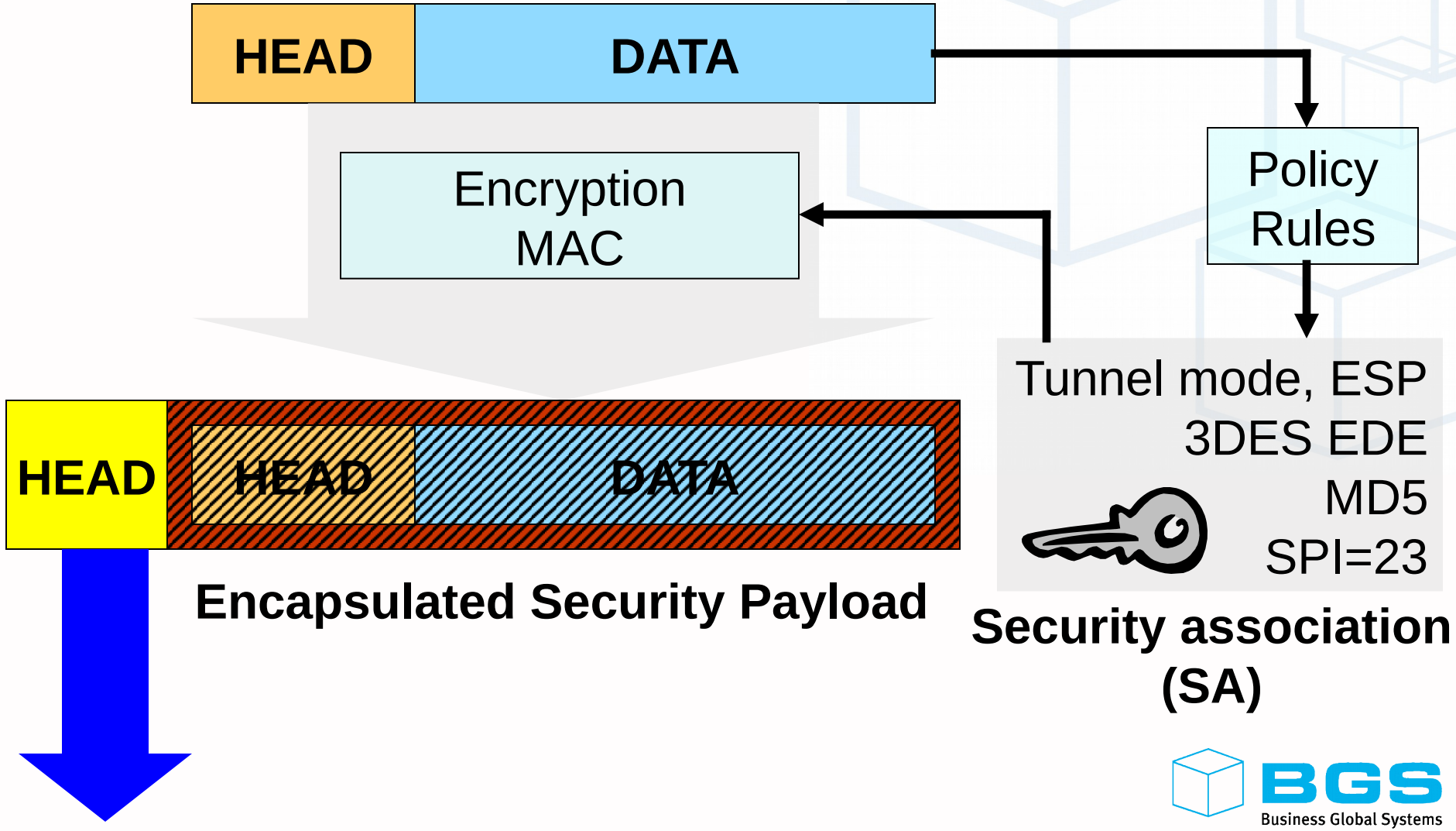


BGS
Business Global Systems

Security gateway

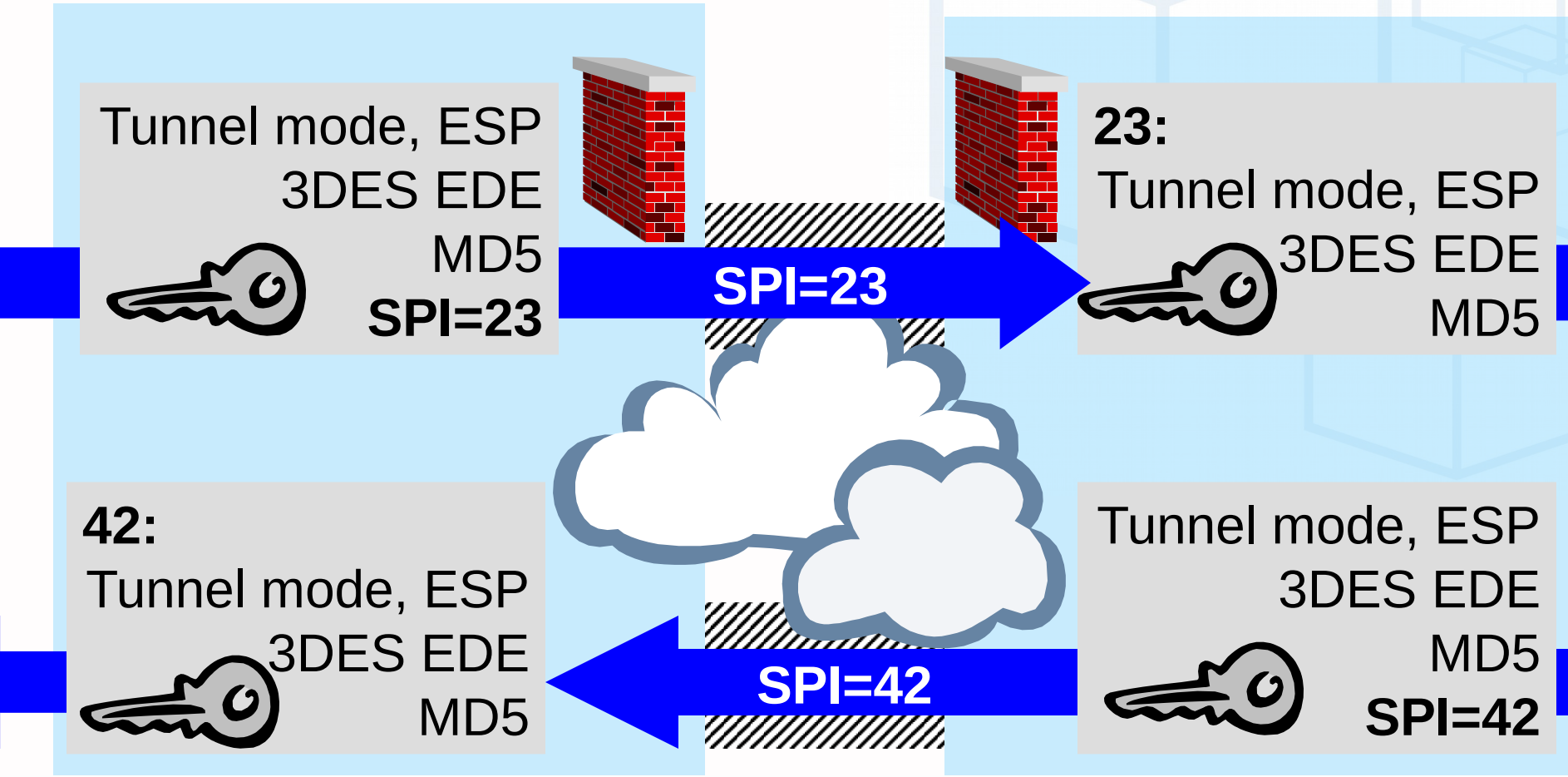


IPsec ESP



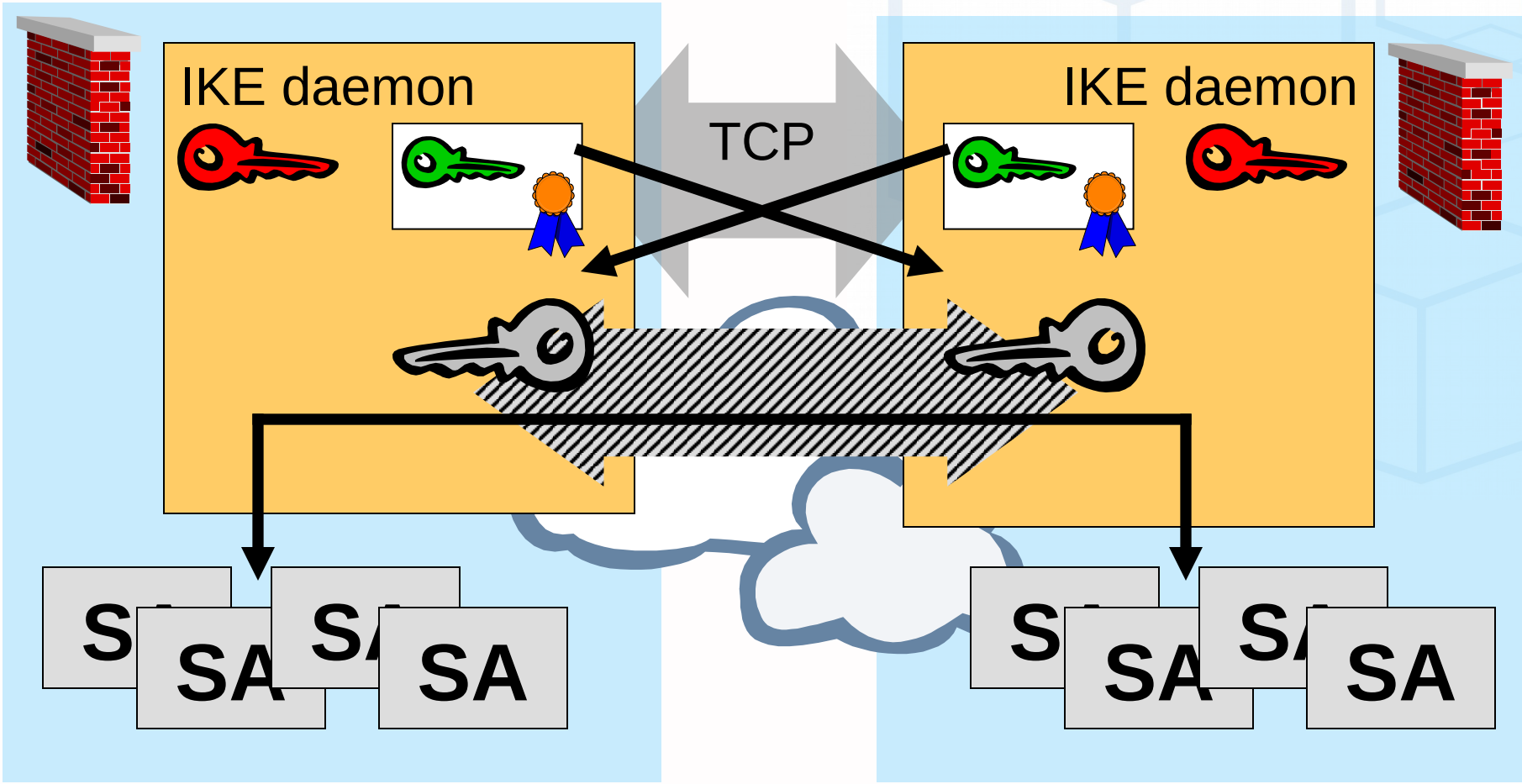
BGS
Business Global Systems

Security association



BGS
Business Global Systems

Internet Key Exchange



IPsec & IKE poznámky

- IPsec ESP & AH
  - ESP - Encapsulated Security Payload
  - AH - Authentication Header
  - ESP & AH processing in kernel
  - Symetric cryptography
- IKE - Internet Key Exchange
  - Asymetric cryptography
  - Processing in user space

IPsec future

- Cisco, Lucent, SUN, Microsoft, ….
  - interoperability
- IPv4 … optional
- IPv6 … integral part

Agenda

- Úvod
- Access control
- Kryptografické protokoly
- VPN
- Záver

(Konečne!)

BGS
Business Global Systems

Záver

- Firewalling
  - užitočný nástroj, ale len sám nestačí
- Kryptografické protokoly
  - Veľa na výber, nie všetky rovnako vhodné
- X.509
  - Infraštruktúra, policy, poriadok
- No more Snake Oil, please ...

Otázky?

BGS
Business Global Systems

Ďakujem za pozornosť

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

BGS
Business Global Systems