Datové schránky „ante portas“

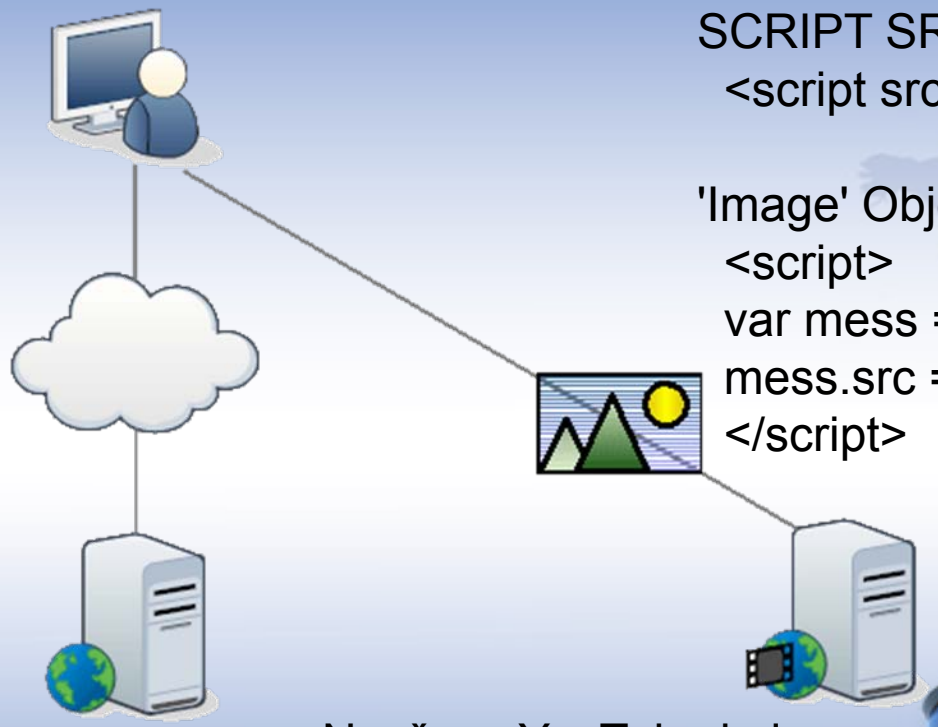
tak „Nepropadejte panice!“

Bezpečnost poprvé

Kernun

CSRF/XSRF

CSRF/XSRF



SCRIPT SRC

```
<script src="http://host/?command">
```

'Image' Object

```
<script>
var mess = new Image();
mess.src = "http://host/?command";
</script>
```

Např. na YouTube byl zranitelný každý formulář, který jsme testovali…

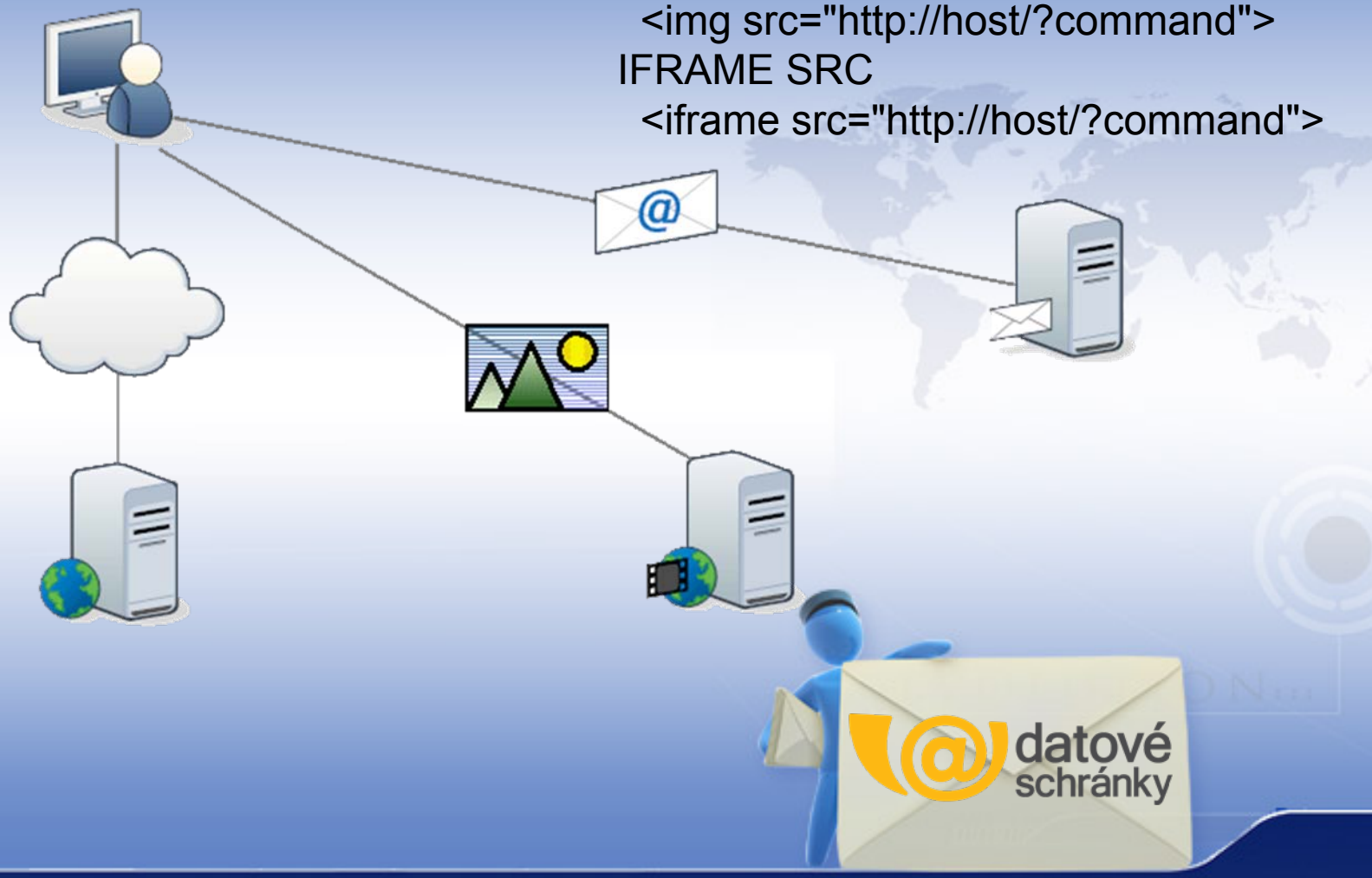
CSRF/XSRF

IMG SRC

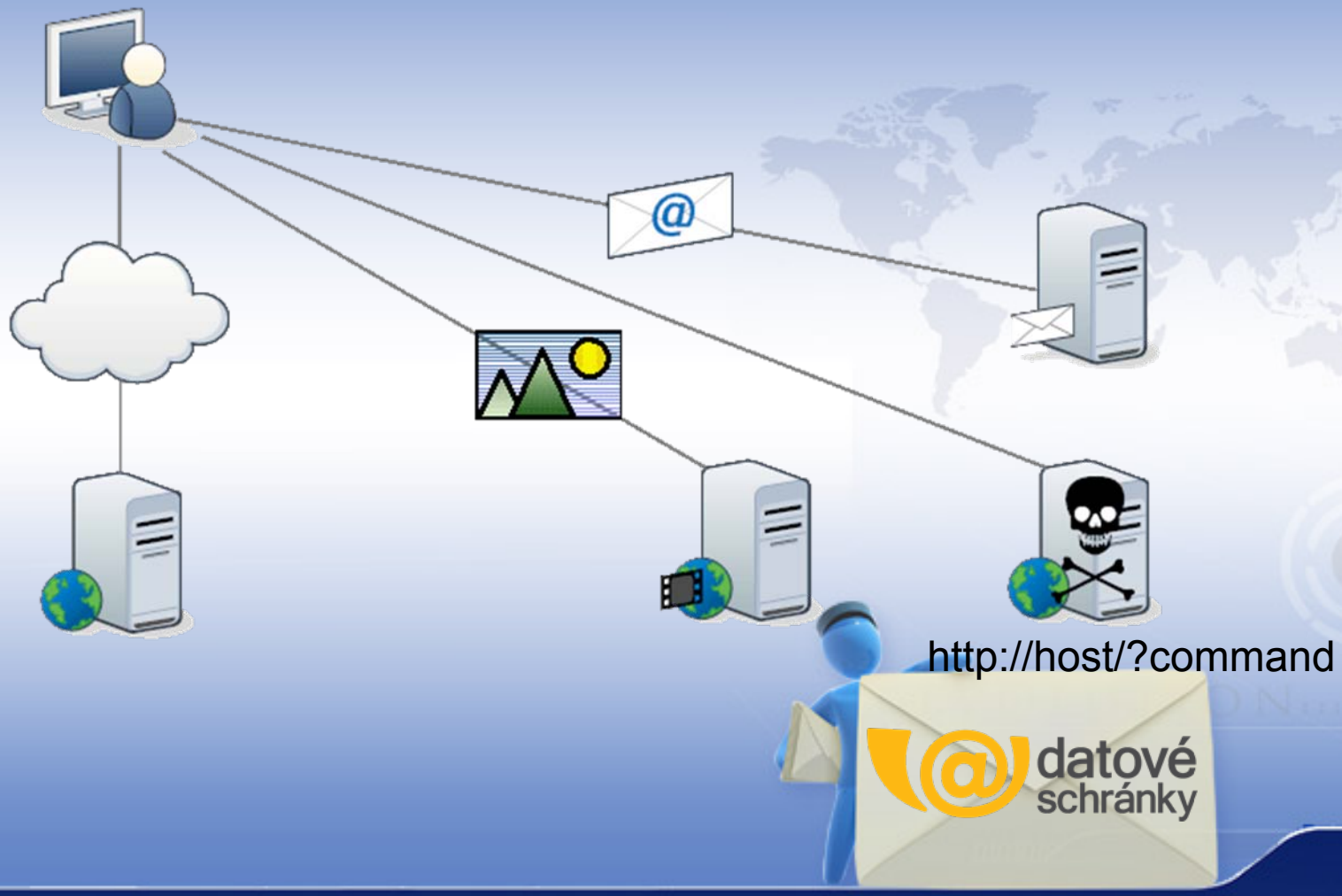
```
<img src="http://host/?command">
```

IFRAME SRC

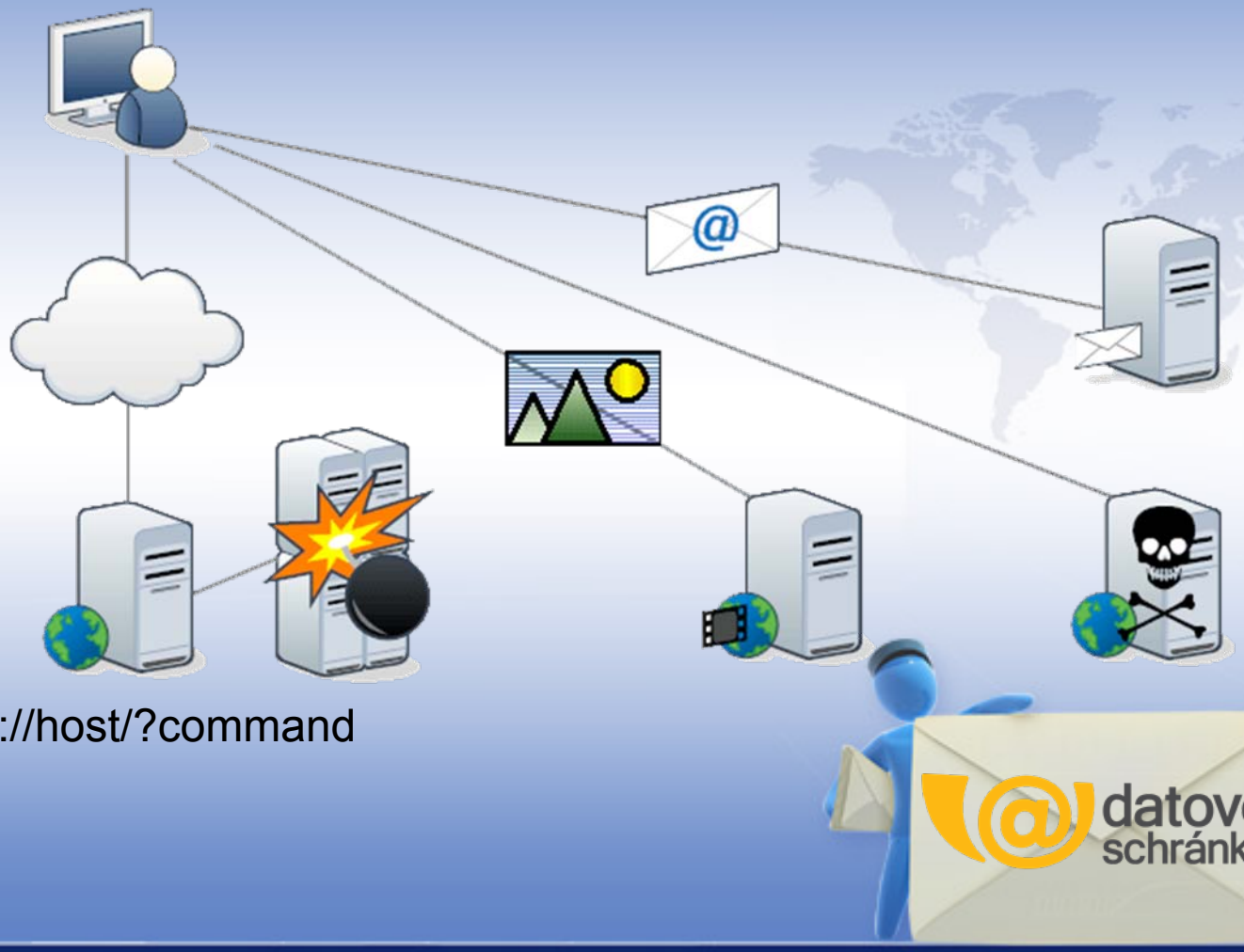
```
<iframe src="http://host/?command">
```



CSRF/XSRF



CSRF/XSRF



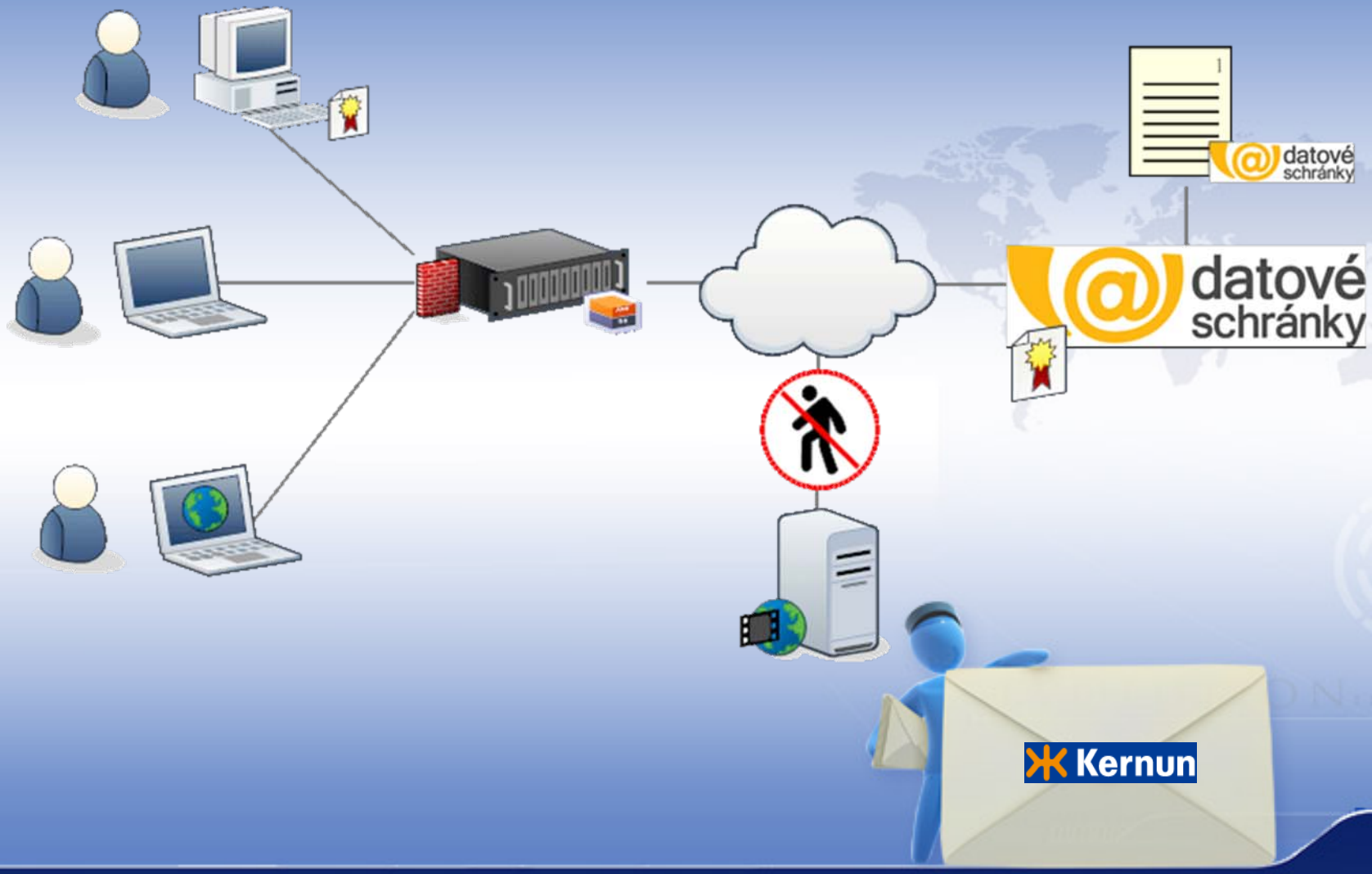
http://host/?command

CSFR/XSFR

- Je to omezeno na HTML?
- Vůbec ne, lze zneužít MS Word dokument, video formáty, flashe, RSS nebo Atom, XML dokumenty a parsery.
- Nezáleží na tom, jestli server používá pouze POST nebo i GET.

ISDS proti CSRF/XSRF

Žádná souběžná připojení



Bezpečnost podruhé

Kernun

Phishing

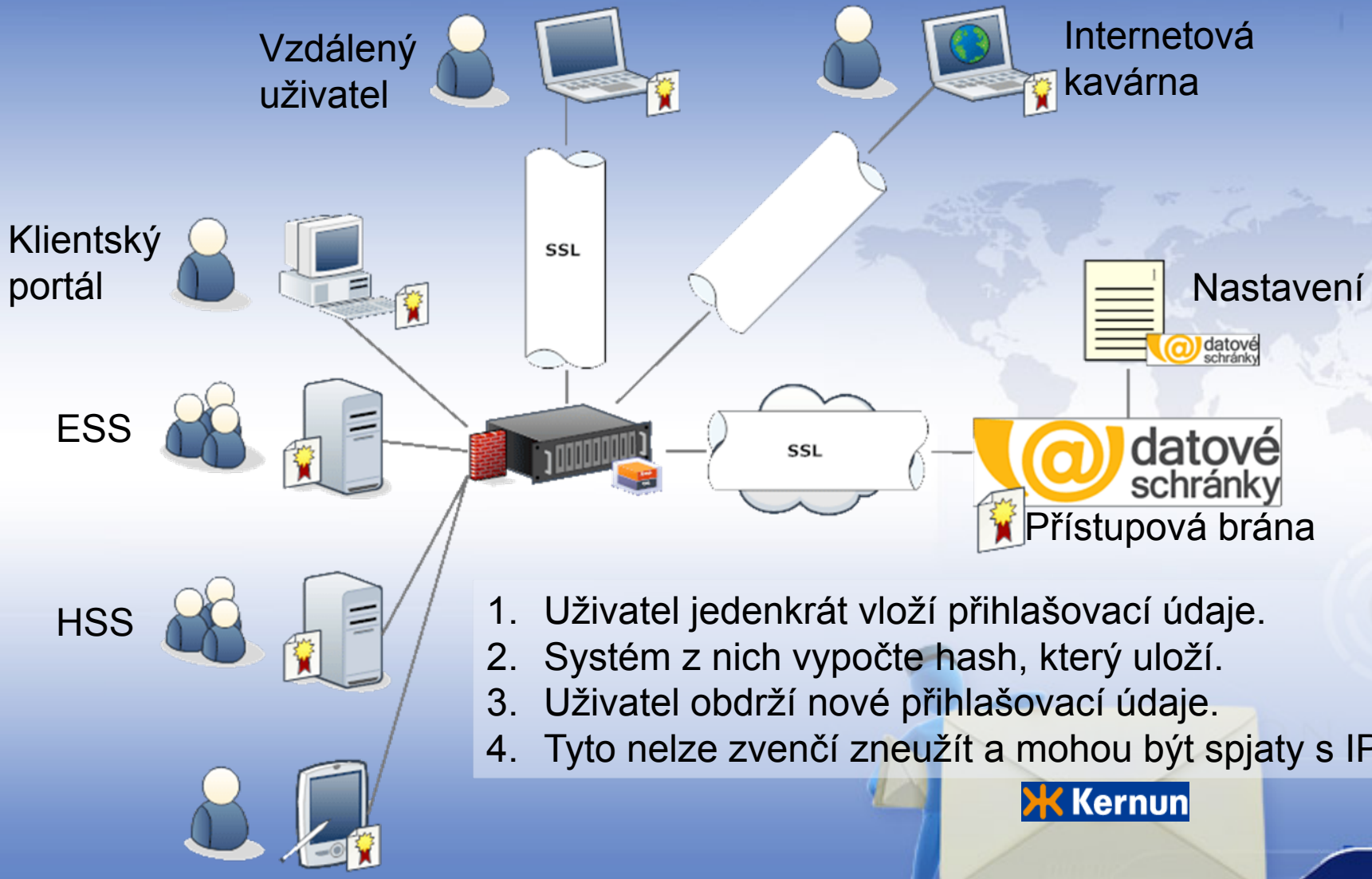
- Prokazujeme se systémovým certifikátem
- E-mailové notifikace jsou podepsány
- Notifikační servery mají nastaveno SPF
- Připravujeme implementaci DNSSEC
- Všechny zprávy mají vzor v dokumentaci
- Informace o posledním přihlášení k systému
- Vzdělávací anti-phishingová hra

Filip versus Rhybáři

192.148.221.13/www.moje datovaschranka.cz

/www.moje dat0vaschranka.cz/login.html

Odstranění rizika phishingu



1. Uživatel jedenkrát vloží přihlašovací údaje.
2. Systém z nich vypočte hash, který uloží.
3. Uživatel obdrží nové přihlašovací údaje.
4. Tyto nelze zvenčí zneužít a mohou být spjaty s IP.

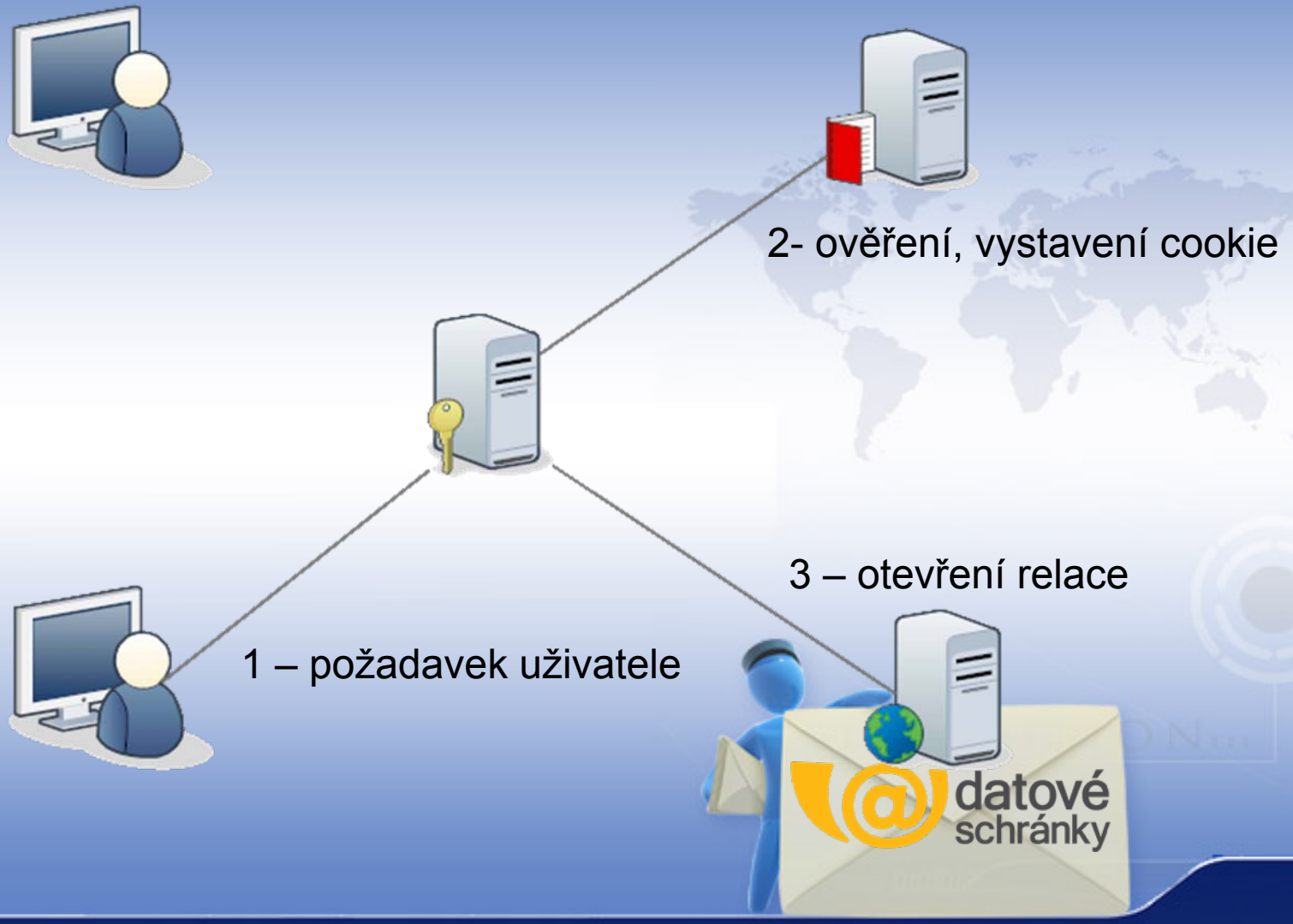
Kernun

Odstranění phishingové pošty

- Reaguje na skutečnost, že všechny e-mailové notifikace ISDS jsou digitálně podepsány a odchozí server má nastaveno SPF:
  - Odstraní e-maily bez platného podpisu
  - Odstraní e-maily s jinou než definovanou trasou doručení (obálka vs. zpráva)

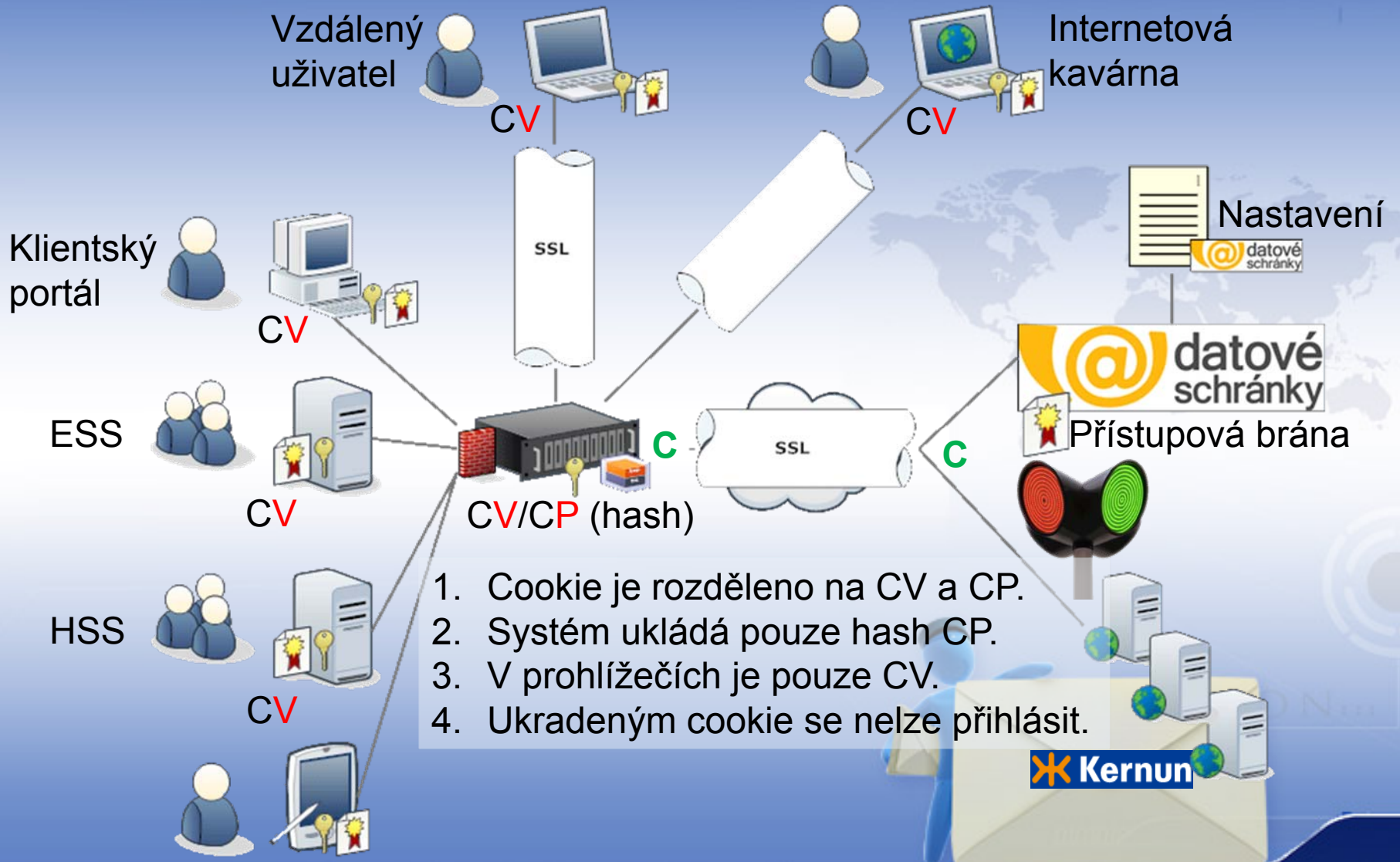
Bezpečnost potřetí

Ukradení relace



Ukradení relace

Žádné ukradené relace



Bezpečnost počtvrté

Kernun

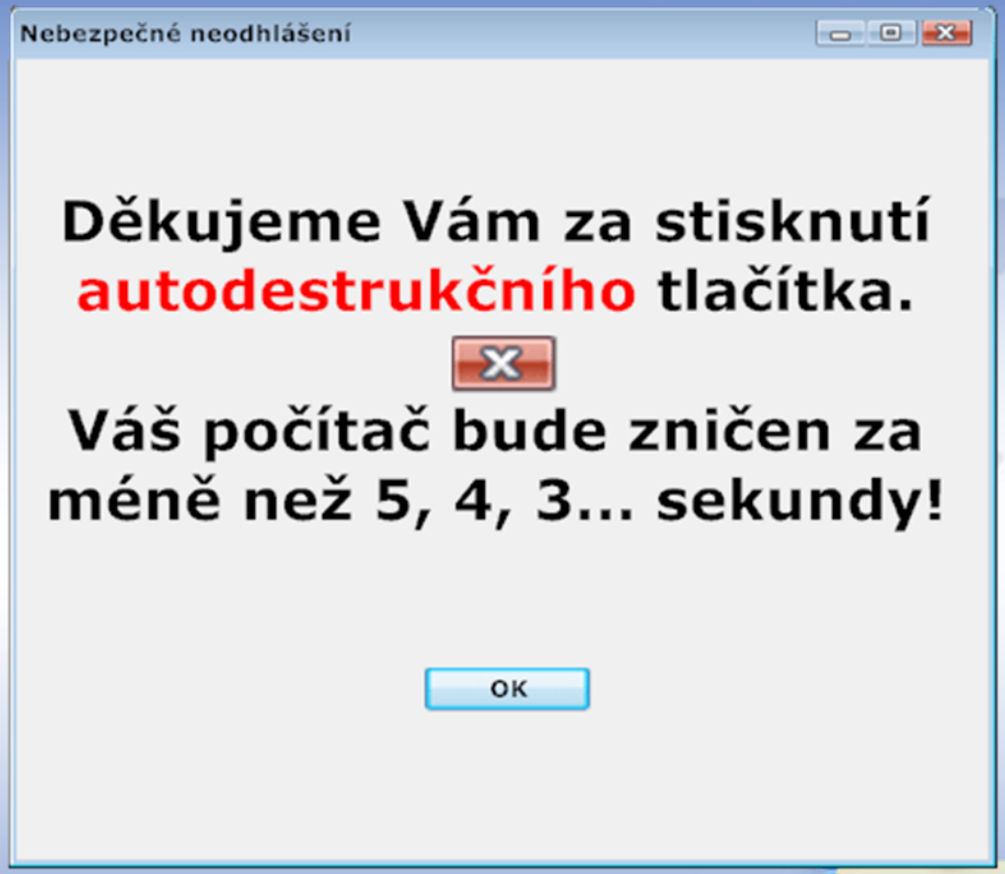
Bezpečnost prohlížečů

- Ukončete všechna připojení k internetu
- Vždy se přihlašujte z nové instance prohlížeče
- Nikdy nepoužívejte paralelní práci v panelech
- Vždy se korektně odhlašujte pomocí tlačítka „Odhlásit“

Autodestrukční tlačítko

datové schránky

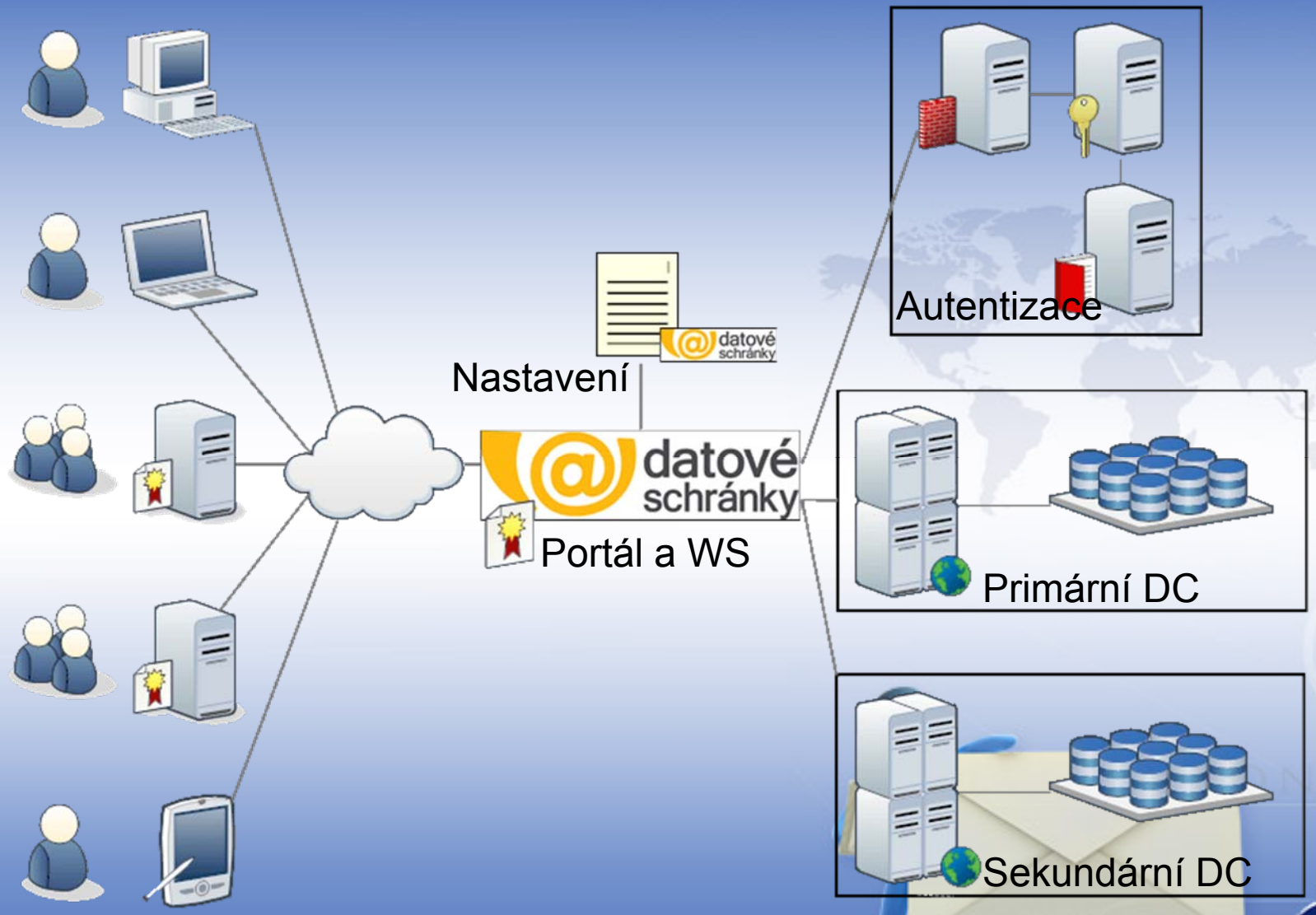
Autodestrukční tlačítko



datové schránky

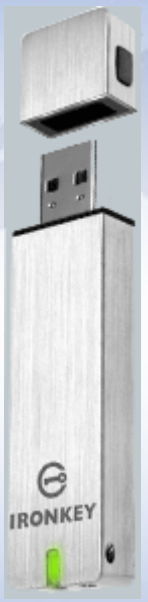
Bezpečnost popáté

Přihlašování do ISDS



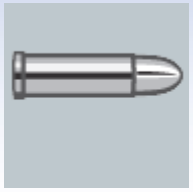
Doporučené připojení k portálu

- Použití komerčního certifikátu pro přístup
  - Uložení v technickém prostředku
    - Příklad: IronKey Personal S200
    - HW šifrování AES 256-bitů
    - Kapacita až 16GB
    - Čtení 30MB/s – zápis 28MB/s
    - Vzdálená správa
    - Aktivní obrana proti kódům

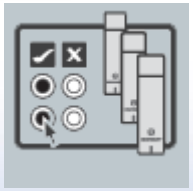


Doporučené připojení ESS/HSS

- Vzdálená správa úložišť certifikátů



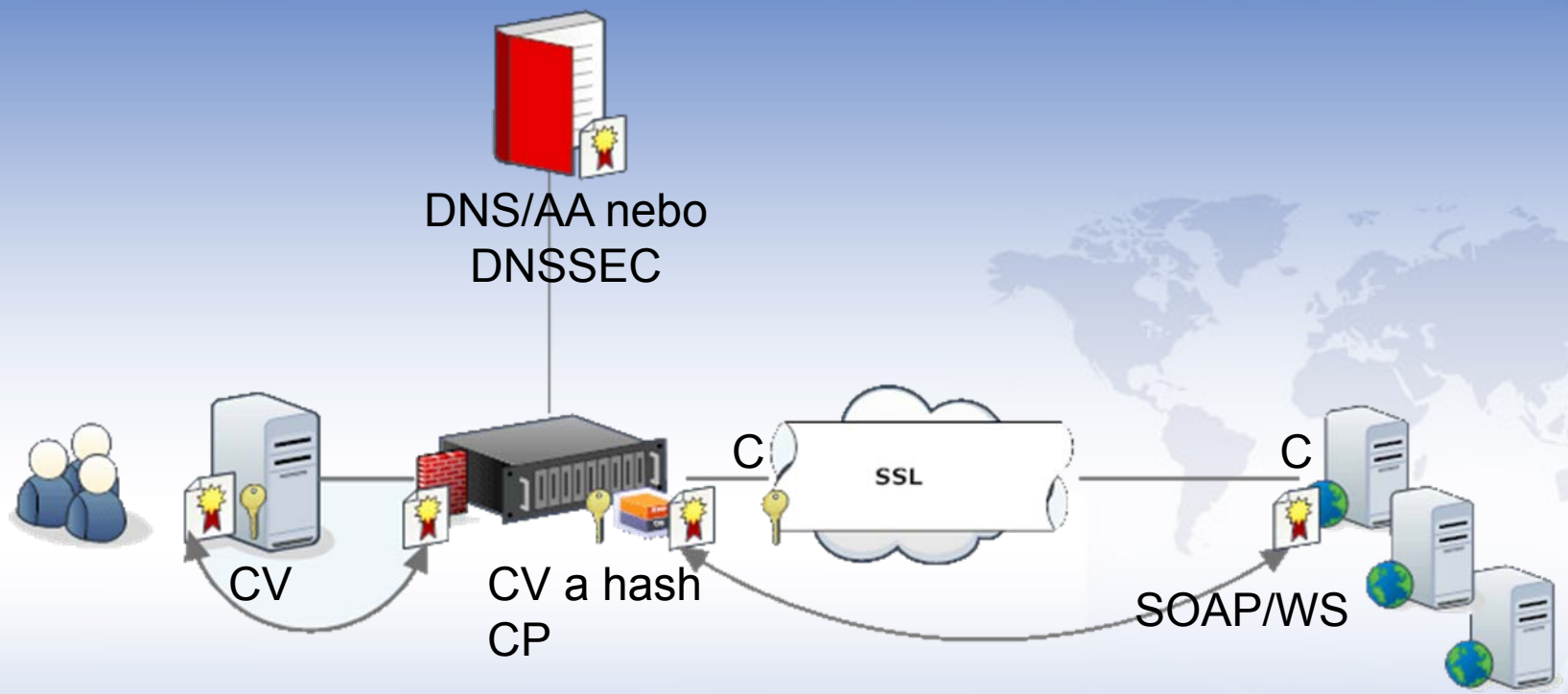
- Zničení ukradených či ztracených



- Připojení výlučně k podnikovým PC

- Virtuální desktop pro vzdálené uživatele

Vlastní certifikační autorita



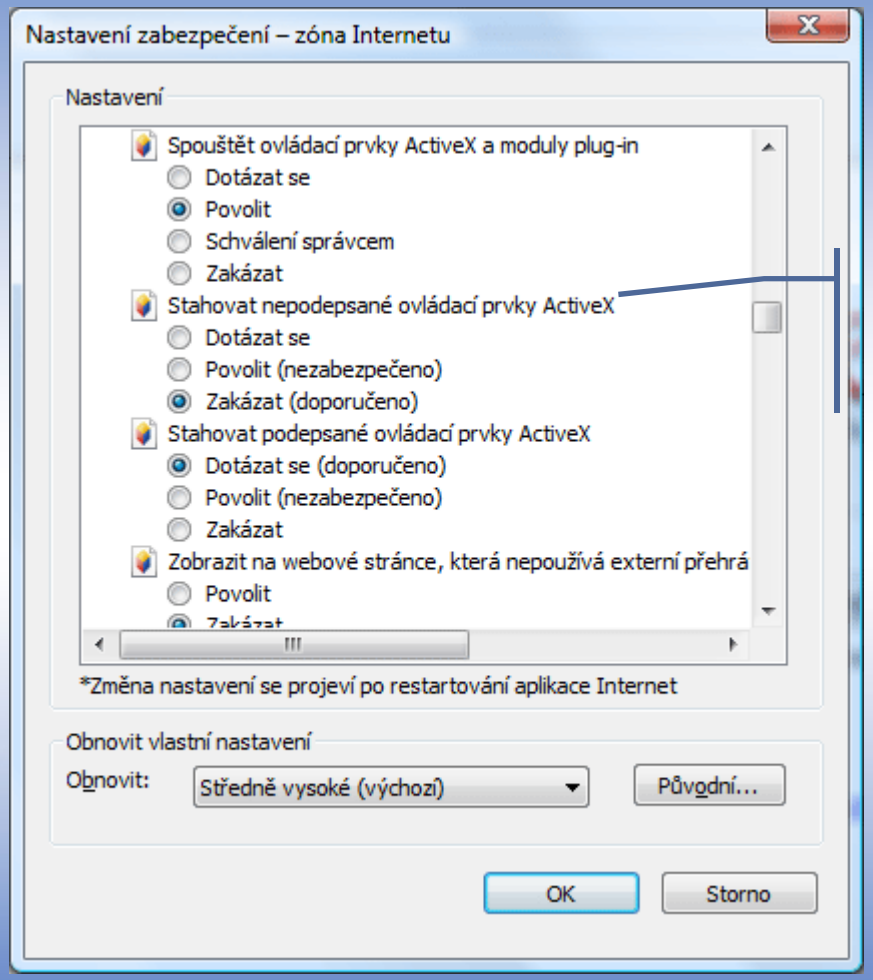
1. Systém pracuje jako certifikační autorita.
2. Klient/server dostávají vlastní certifikát od proxy.
3. HTTP proxy umí dešifrovat/zašifrovat SSL.
4. Ostrý certifikát je odesílán z bezpečného keystore.
5. „Server-Cert-Match_Domain“ kontroluje shodu.

Bezpečnost pošesté

Formát datové zprávy

datové schránky

Bezpečnost plug-inu

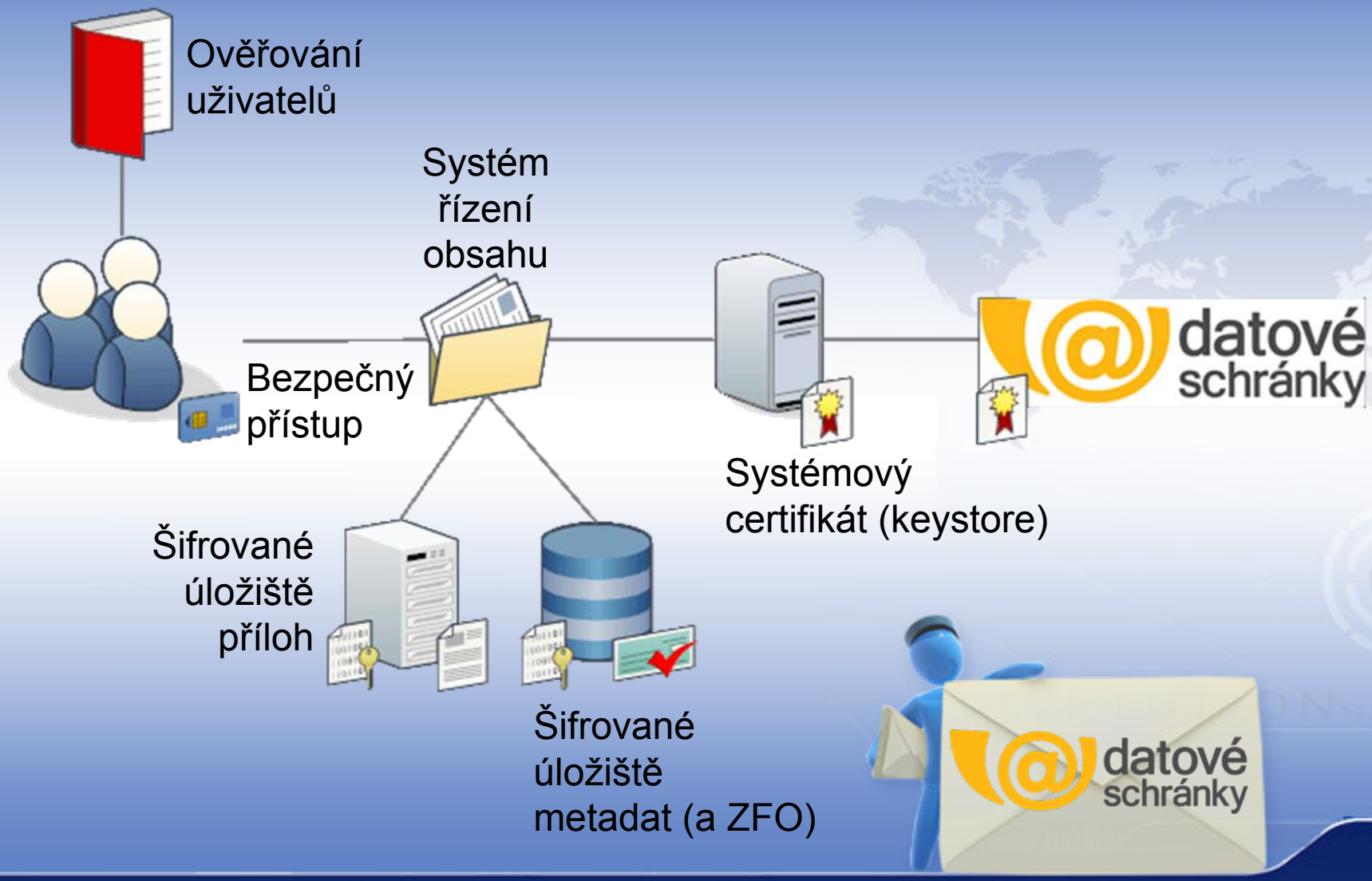


Zakázat stahování nepodepsaných ActiveX prvků (doporučeno)

602XML Filler 2

Účelem filleru není číst formuláře, ale ukládat zprávy pro institucionální archív

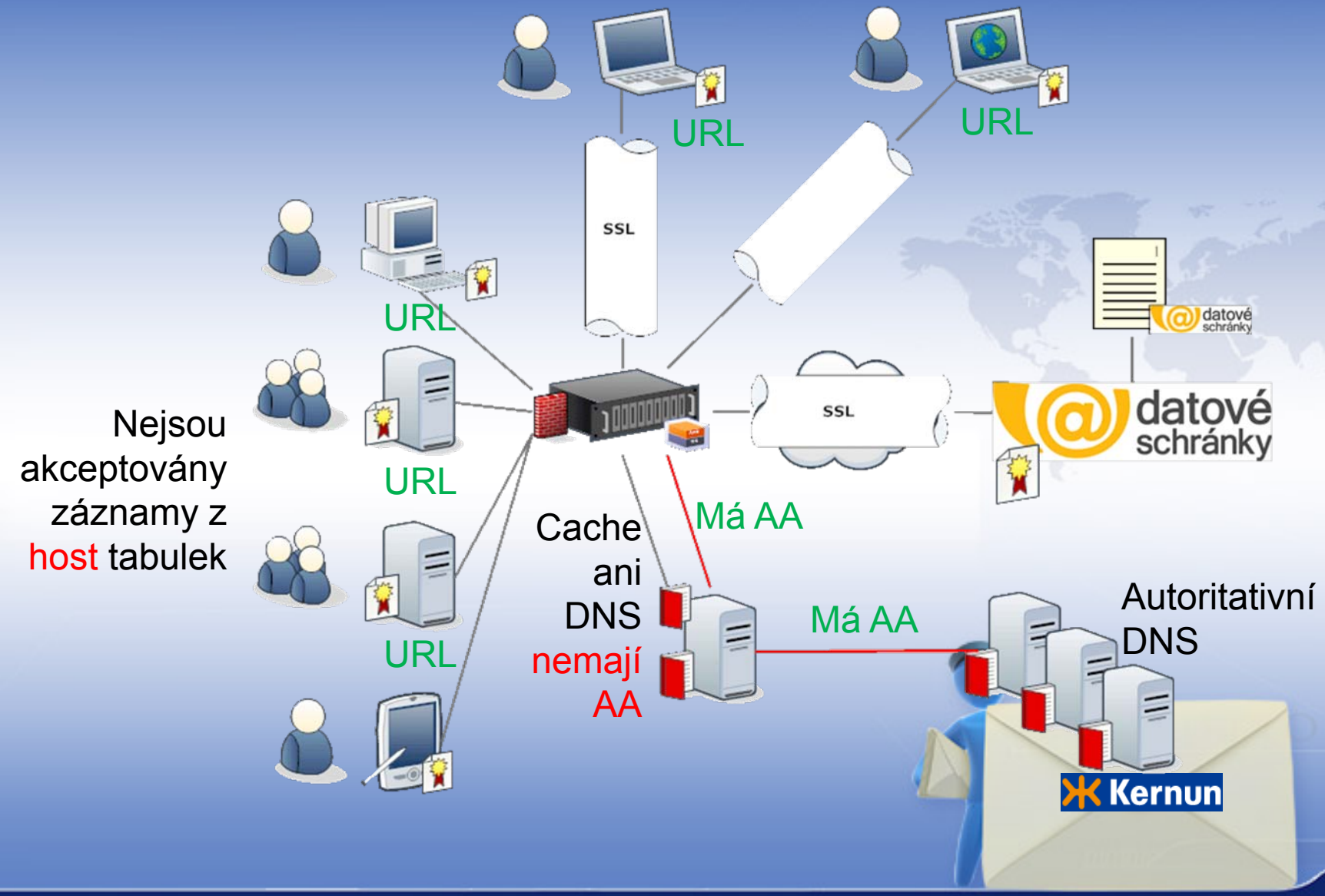
Bezpečnost aplikací 3. stran



Bezpečnost posedmé

Kernun

Autoritativní DNS



Kontakt

Radek Smolík
Bezpečnostní architekt
+420 606 655 625
smolikr@e-trends.cz