

# Digitálny podpis

Michal Mikuš

michalmikus@yahoo.co.uk

26.11.2015



# Kto som

- 1998-2002 GJH, (KMS, KSP, FKS),
- 2002-2007 FMFI UK (KMS),
- 2007-2013 doktorand FEI STU,
- 2013- SW analytik (Ditec).



# O čom to dnes bude

## Digitálne podpisy:

- princíp,
- potrebné nástroje,
- fungovanie,
- ukážka.



# O čom to dnes bude

## Digitálne podpisy:

- princíp,
- potrebné nástroje,
- fungovanie,
- ukážka.



# O čom to dnes bude

## Digitálne podpisy:

- princíp,
- potrebné nástroje,
- fungovanie,
- ukážka.



# O čom to dnes bude

## Digitálne podpisy:

- princíp,
- potrebné nástroje,
- fungovanie,
- ukážka.



# O čom to dnes bude

## Digitálne podpisy:

- princíp,
- potrebné nástroje,
- fungovanie,
- ukážka.



# Šifrovacie schémy

Šifra je spôsob:

- ako zašifrovať správu  $m$ :  $m \rightarrow c$ ,
- a ako ju korektne dešifrovať:  $c \rightarrow m$ .

Podľa toho, ako sa to deje, delíme šifry na klasické a moderné.  
Tie moderné delíme na symetrické a asymetrické.





# Šifrovacie schémy

Šifra je spôsob:

- ako zašifrovať správu  $m$ :  $m \rightarrow c$ ,
- a ako ju korektne dešifrovať:  $c \rightarrow m$ .

Podľa toho, ako sa to deje, delíme šifry na klasické a moderné.  
Tie moderné delíme na symetrické a asymetrické.



# Šifrovacie schémy

Šifra je spôsob:

- ako zašifrovať správu  $m$ :  $m \rightarrow c$ ,
- a ako ju korektne dešifrovať:  $c \rightarrow m$ .

Podľa toho, ako sa to deje, delíme šifry na klasické a moderné.  
Tie moderné delíme na symetrické a asymetrické.



# Šifrovacie schémy

Šifra je spôsob:

- ako zašifrovať správu  $m$ :  $m \rightarrow c$ ,
- a ako ju korektne dešifrovať:  $c \rightarrow m$ .

Podľa toho, ako sa to deje, delíme šifry na klasické a moderné.  
Tie moderné delíme na symetrické a asymetrické.



# Šifrovacie schémy

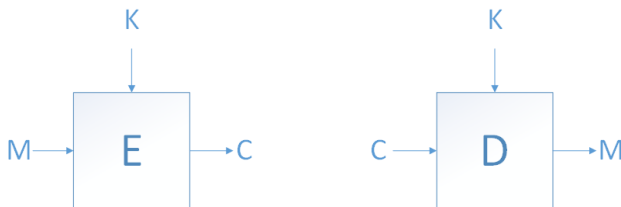
Šifra je spôsob:

- ako zašifrovať správu  $m$ :  $m \rightarrow c$ ,
- a ako ju korektne dešifrovať:  $c \rightarrow m$ .

Podľa toho, ako sa to deje, delíme šifry na klasické a moderné.  
Tie moderné delíme na symetrické a asymetrické.

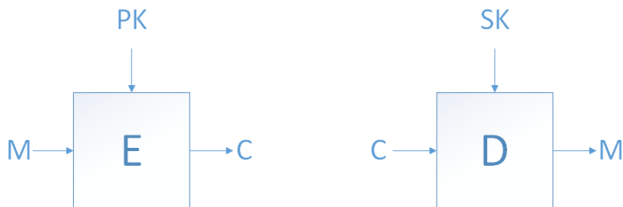


# Symetrické šifry



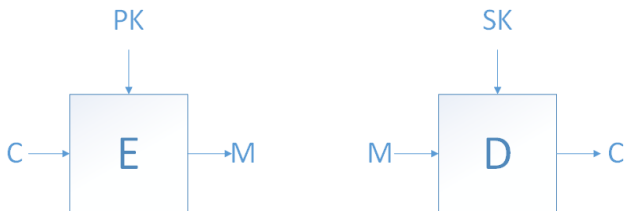
- rýchle,
- bezpečné už pre  $|K| = 256$  bitov,
- problém je v distribúcii kľúčov,
- napr. Caesar, Vigenere, Vernam, A5, AES, GOST, BlowFish, TwoFish.

# Asymetrické šifry



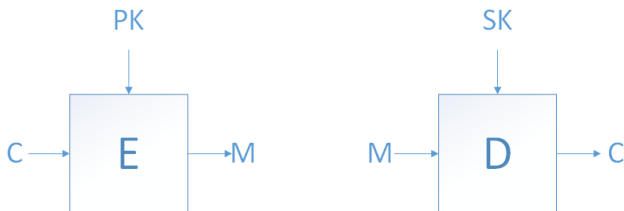
- pomalšie,
- bezpečné pre  $|K| \approx 1024$  bitov,
- bezpečnosť je na ťažkých problémoch,
- napr. RSA, ElGamal, McEliece, NTRU, Rabin, Paillier.

# Schéma digitálneho podpisu



- "otočená asymetrická šifra"
- *D* bude slúžiť na podpis:
  - držiteľ *sk* podpíše správu *M*,
  - hocikto (kto má *pk*) vie overiť,

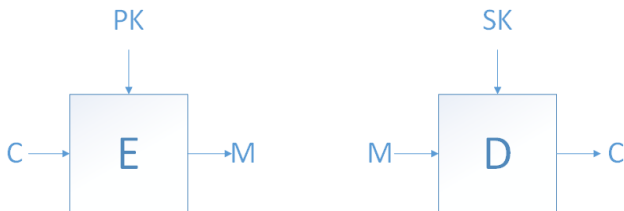
# Schéma digitálneho podpisu



- "otočená asymetrická šifra"
- $D$  bude slúžiť na podpis:
  - držiteľ  $sk$  podpíše správu  $M$ ,
  - hocikto (kto má  $pk$ ) vie overiť,

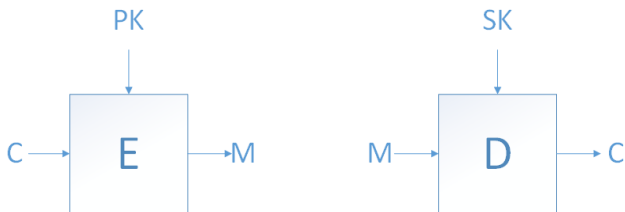


# Schéma digitálneho podpisu



- "otočená asymetrická šifra"
- $D$  bude slúžiť na podpis:
  - držiteľ  $sk$  podpíše správu  $M$ ,
  - hocikto (kto má  $pk$ ) vie overiť,

# Schéma digitálneho podpisu



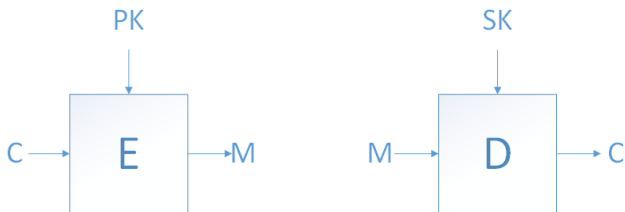
## Podrobnejšie:

- podpísanie:  $S = D(M, sk)$
- overenie:  $E(S, pk) = M'$
- viem, že  $E(D(M, sk), pk) = M$

Takže celý postup overenia je  $E(S, pk) \stackrel{?}{=} M$ , ak áno, tak platí.



# Schéma digitálneho podpisu



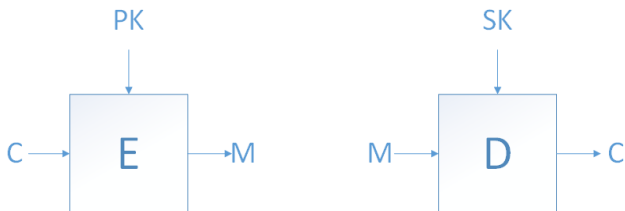
Podrobnejšie:

- podpísanie:  $S = D(M, sk)$
- overenie:  $E(S, pk) = M'$
- viem, že  $E(D(M, sk), pk) = M$

Takže celý postup overenia je  $E(S, pk) \stackrel{?}{=} M$ , ak áno, tak platí.



# Schéma digitálneho podpisu



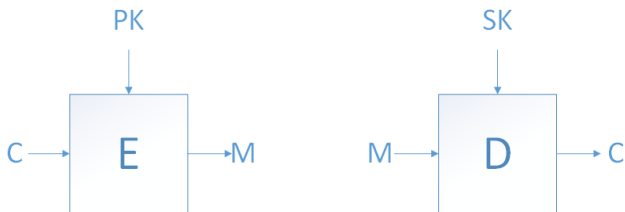
Podrobnejšie:

- podpísanie:  $S = D(M, sk)$
- overenie:  $E(S, pk) = M'$
- viem, že  $E(D(M, sk), pk) = M$

Takže celý postup overenia je  $E(S, pk) \stackrel{?}{=} M$ , ak áno, tak platí.



# Schéma digitálneho podpisu



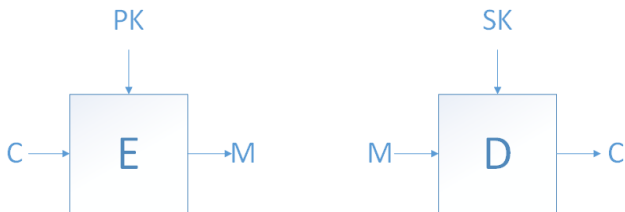
Podrobnejšie:

- podpísanie:  $S = D(M, sk)$
- overenie:  $E(S, pk) = M'$
- viem, že  $E(D(M, sk), pk) = M$

Takže celý postup overenia je  $E(S, pk) \stackrel{?}{=} M$ , ak áno, tak platí.



# Schéma digitálneho podpisu



Podrobnejšie:

- podpísanie:  $S = D(M, sk)$
- overenie:  $E(S, pk) = M'$
- viem, že  $E(D(M, sk), pk) = M$

Takže celý postup overenia je  $E(S, pk) \stackrel{?}{=} M$ , ak áno, tak platí.



# Pod'me začať

- vezmime si RSA,
- vygenerujeme kľúče,
  - ako podpísať moju esež z AJ?
  - ako bude vôbec p.profesor vedieť, čo sa nezmysel som mu poslal?
  - ako bude p.profesor vedieť, že je moja?



# Pod'me začať

- vezmime si RSA,
- vygenerujeme kľúče,
  - ako podpísať moju esež z AJ?
  - ako bude vôbec p.profesor vedieť, čo sa nezmysel som mu poslal?
  - ako bude p.profesor vedieť, že je moja?





# Ako podpísať?

Vždy podpíšem len *odtlačok* dokumentu.

Hašovacie funkcie:

- zobrazia ľubovoľne dlhý reťazec na reťazec určitej dĺžky (256 bitov),
- urobia to dobre:
  - z odtlačku sa nedá spočítať správa,
  - rôzne správy budú mať rôzne odtlačky.

Spotrebný tovar. Životnosť býva 0-15 rokov.



# Ako podpísať?

Vždy podpíšem len *odtlačok* dokumentu.

Hašovacie funkcie:

- zobrazia ľubovoľne dlhý reťazec na reťazec určitej dĺžky (256 bitov),
- urobia to dobre:
  - z odtlačku sa nedá spočítať správa,
  - rôzne správy budú mať rôzne odtlačky.

Spotrebný tovar. Životnosť býva 0-15 rokov.



# Ako podpísať?

Vždy podpíšem len *odtlačok* dokumentu.

Hašovacie funkcie:

- zobrazia ľubovoľne dlhý reťazec na reťazec určitej dĺžky (256 bitov),
- urobia to dobre:
  - z odtlačku sa nedá spočítať správa,
  - rôzne správy budú mať rôzne odtlačky.

Spotrebný tovar. Životnosť býva 0-15 rokov.



# Ako podpísať?

Vždy podpíšem len *odtlačok* dokumentu.

Hašovacie funkcie:

- zobrazia ľubovoľne dlhý reťazec na reťazec určitej dĺžky (256 bitov),
- urobia to dobre:
  - z odtlačku sa nedá spočítať správa,
  - rôzne správy budú mať rôzne odtlačky.

Spotrebný tovar. Životnosť býva 0-15 rokov.



# Ako podpísať?

Vždy podpíšem len *odtlačok* dokumentu.

Hašovacie funkcie:

- zobrazia ľubovoľne dlhý reťazec na reťazec určitej dĺžky (256 bitov),
- urobia to dobre:
  - z odtlačku sa nedá spočítať správa,
  - rôzne správy budú mať rôzne odtlačky.

Spotrebný tovar. Životnosť býva 0-15 rokov.



# Ako podpísať?

Vždy podpíšem len *odtlačok* dokumentu.

Hašovacie funkcie:

- zobrazia ľubovoľne dlhý reťazec na reťazec určitej dĺžky (256 bitov),
- urobia to dobre:
  - z odtlačku sa nedá spočítať správa,
  - rôzne správy budú mať rôzne odtlačky.

Spotrebný tovar. Životnosť býva 0-15 rokov.



# Ako bude ten druhý vedieť, čo to je?

## Formát podpisu:

- schéma, ako taký podpis vyzerá,
- umožňuje ľahké používanie,
- najlepšie by bolo mať celosvetový formát,
- máme taký európsky (dokonca niekoľko),
- CMS, XML, Pdf.



# Formát XAdES

- založený na XMLDSIG (formát z roku 2000), detaily na [https://en.wikipedia.org/wiki/XML\\_Signature](https://en.wikipedia.org/wiki/XML_Signature),
- definovaný v ETSI (<http://www.etsi.org/standards>),

```
<Signature>
  <SignedInfo>
    <CanonicalizationMethod />
    <SignatureMethod />
    <Reference>
      <Transforms>
      <DigestMethod>
      <DigestValue>
    </Reference>
    <Reference /> etc.
  </SignedInfo>
  <SignatureValue />
  <KeyInfo />
  <Object />
</Signature>
```





# Ako viem, kto je autor podpisu?

Kľúče a identity. Spája ich *certifikát*:

- kto som (číslo OP nie, napr. rodné číslo),
- aký je môj verejný kľúč,
- aká je jeho platnosť (od,do),
- kto mi ho vydal (CA),
- podpis toho, kto mi ho vydal.



# Ako viem, kto je autor podpisu?

Kľúče a identity. Spája ich *certifikát*:

- kto som (číslo OP nie, napr. rodné číslo),
- aký je môj verejný kľúč,
- aká je jeho platnosť (od,do),
- kto mi ho vydal (CA),
- podpis toho, kto mi ho vydal.



# Ako viem, kto je autor podpisu?

Kľúče a identity. Spája ich *certifikát*:

- kto som (číslo OP nie, napr. rodné číslo),
- aký je môj verejný kľúč,
- aká je jeho platnosť (od,do),
- kto mi ho vydal (CA),
- podpis toho, kto mi ho vydal.



# Ako viem, kto je autor podpisu?

Kľúče a identity. Spája ich *certifikát*:

- kto som (číslo OP nie, napr. rodné číslo),
- aký je môj verejný kľúč,
- aká je jeho platnosť (od,do),
- kto mi ho vydal (CA),
- podpis toho, kto mi ho vydal.



# Ako viem, kto je autor podpisu?

Kľúče a identity. Spája ich *certifikát*:

- kto som (číslo OP nie, napr. rodné číslo),
- aký je môj verejný kľúč,
- aká je jeho platnosť (od,do),
- kto mi ho vydal (CA),
- podpis toho, kto mi ho vydal.



# Ako viem, kto je autor podpisu?

Kľúče a identity. Spája ich *certifikát*:

- kto som (číslo OP nie, napr. rodné číslo),
- aký je môj verejný kľúč,
- aká je jeho platnosť (od,do),
- kto mi ho vydal (CA),
- podpis toho, kto mi ho vydal.



# Hierarchia certifikátov

- každý certifikát má vydavateľa . . . hm,
- rekurzívny problém,
- navrchu je certifikát, ktorý podpísal sám seba,
- tu v SR je to KCA3 od NBÚ.



# Hierarchia certifikátov

- každý certifikát má vydavateľa . . . hm,
- rekurzívny problém,
- navrchu je certifikát, ktorý podpísal sám seba,
- tu v SR je to KCA3 od NBÚ.





# Hierarchia certifikátov

- každý certifikát má vydavateľa . . . hm,
- rekurzívny problém,
- navrchu je certifikát, ktorý podpísal sám seba,
- tu v SR je to KCA3 od NBÚ.



# Hierarchia certifikátov

- každý certifikát má vydavateľa . . . hm,
- rekurzívny problém,
- navrchu je certifikát, ktorý podpísal sám seba,
- tu v SR je to KCA3 od NBÚ.



# Hierarchia certifikátov, koreň

Ako sa zaručí bezpečnosť koreňa celého stromu?

INFOFORMIZÁCIA - Slovensko x Koreňová certifikačná autorita x MD 398: Signature Syntax and ... x certias - How do I put test ... x ETSI - ICT Standards, GM ...

www.nbusr.sk/sk/elektronicky-podpis/korenova-certifikacne-autorita-kca.1.html

SLOVENSKY | ENGLISH

Kontakty | Štruktúra úradu | Technický prevádzkovateľ | Dátum poslednej aktualizácie: 25.11.2015

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

— O ÚRADE —

OCHRANA UTAJOVANÝCH SKUTOČNOSTÍ

ŠÍFROVÁ OCHRANA INFORMÁCIÍ

ELEKTRONICKÝ PODPIS

PRÁVNE PREDPISY

Neprehliadnite

Osobný dotazník osoby

Bezpečnostný dotazník osoby

Návod na vyplnenie niektorých bodov bezpečnostného dotazníka

Bezpečnostný dotazník podnikateľa platný od 1.

ELEKTRONICKÝ PODPIS | KOREŇOVÁ CERTIFIKAČNÁ AUTORITA (KCA)

- [sp.nbusr.sk](http://sp.nbusr.sk)

Oznamy KCA

Self-signed certifikát verejného kľúča KCA3 (následníka KCA2) bol v zmysle § 12 ods. 2 vyhlášky NBÚ č. 135/2009 Z.z. zverejnený v tlačí:

- Hospodárske noviny, dňa 19. novembra 2009, konkrétne na 4. strane
- Verejná správa, číslo 25-26/2009, konkrétne na 45. strane

Start | [Icons] | 23:02 | 25.11.2015

# A prečo by to malo fungovať?

Musia byť definované pravidlá, že profesori na GJH budú uznávať aj eseje podpísané dig. podpisom (a hlavne za akých podmienok).

Sú tu slovenské:

- zákon č.215 z 15. marca 2002 o elektronickom podpise,
- výnos MFSR zo 4. marca 2014, o štandardoch pre informačné systémy verejnej správy,
- vyhlášky NBÚ č.131 až 136.

A sú tu európske:

- Rozhodnutie č.148/2014,
- Nariadenie EP A RADY (EÚ) č. 910/2014,
- Rozhodnutie č.296/2015,



# A prečo by to malo fungovať?

Musia byť definované pravidlá, že profesori na GJH budú uznávať aj eseje podpísané dig. podpisom (a hlavne za akých podmienok).

Sú tu slovenské:

- zákon č.215 z 15. marca 2002 o elektronickom podpise,
- výnos MFSR zo 4. marca 2014, o štandardoch pre informačné systémy verejnej správy,
- vyhlášky NBÚ č.131 až 136.

A sú tu európske:

- Rozhodnutie č.148/2014,
- Nariadenie EP A RADY (EÚ) č. 910/2014,
- Rozhodnutie č.296/2015,



# A prečo by to malo fungovať?

Musia byť definované pravidlá, že profesori na GJH budú uznávať aj eseje podpísané dig. podpisom (a hlavne za akých podmienok).

Sú tu slovenské:

- zákon č.215 z 15. marca 2002 o elektronickom podpise,
- výnos MFSR zo 4. marca 2014, o štandardoch pre informačné systémy verejnej správy,
- vyhlášky NBÚ č.131 až 136.

A sú tu európske:

- Rozhodnutie č.148/2014,
- Nariadenie EP A RADY (EÚ) č. 910/2014,
- Rozhodnutie č.296/2015,



# Príklad



# Zhnutie

- Čo znamená veriť digitálnemu podpisu?

- veriť hašovacej funkcii,
- veriť asymetrickej šifre,
- veriť certifikátu podpisovateľa.

- Ako ho vytvárať/používať?

- EU projekt:

[https://joinup.ec.europa.eu/asset/sd-dss/asset\\_release/all](https://joinup.ec.europa.eu/asset/sd-dss/asset_release/all)

- Lock It: (Peter Rybár, <http://lockitin.webnode.sk/>),
- slovensko.sk: Aplikácia D.Signer/XAdES.

Treba si zohnať certifikát, alebo eID a čítačku.





# Zhnutie

- Čo znamená veriť digitálnemu podpisu?

- veriť hašovacej funkcii,
- veriť asymetrickej šifre,
- veriť certifikátu podpisovateľa.

- Ako ho vytvárať/používať?

- EU projekt:

[https://joinup.ec.europa.eu/asset/sd-dss/asset\\_release/all](https://joinup.ec.europa.eu/asset/sd-dss/asset_release/all)

- Lock It: (Peter Rybár, <http://lockitin.webnode.sk/>),
- slovensko.sk: Aplikácia D.Signer/XAdES.

Treba si zohnať certifikát, alebo eID a čítačku.



# Zhnutie

- Čo znamená veriť digitálnemu podpisu?

- veriť hašovacej funkcii,
- veriť asymetrickej šifre,
- veriť certifikátu podpisovateľa.

- Ako ho vytvárať/používať?

- EU projekt:

[https://joinup.ec.europa.eu/asset/sd-dss/asset\\_release/all](https://joinup.ec.europa.eu/asset/sd-dss/asset_release/all)

- Lock It: (Peter Rybár, <http://lockitin.webnode.sk/>),
- slovensko.sk: Aplikácia D.Signer/XAdES.

Treba si zohnať certifikát, alebo eID a čítačku.



# Zhnutie

- Čo znamená veriť digitálnemu podpisu?

- veriť hašovacej funkcii,
- veriť asymetrickej šifre,
- veriť certifikátu podpisovateľa.

- Ako ho vytvárať/používať?

- EU projekt:

[https://joinup.ec.europa.eu/asset/sd-dss/asset\\_release/all](https://joinup.ec.europa.eu/asset/sd-dss/asset_release/all)

- Lock It: (Peter Rybár, <http://lockitin.webnode.sk/>),
- slovensko.sk: Aplikácia D.Signer/XAdES.

Treba si zohnať certifikát, alebo eID a čítačku.



# Zhnutie

- Čo znamená veriť digitálnemu podpisu?
  - veriť hašovacej funkcii,
  - veriť asymetrickej šifre,
  - veriť certifikátu podpisovateľa.
- Ako ho vytvárať/používať?

- EU projekt:

[https://joinup.ec.europa.eu/asset/sd-dss/asset\\_release/all](https://joinup.ec.europa.eu/asset/sd-dss/asset_release/all)

- Lock It: (Peter Rybár, <http://lockitin.webnode.sk/>),
- slovensko.sk: Aplikácia D.Signer/XAdES.

Treba si zohnať certifikát, alebo eID a čítačku.



# Zhnutie

- Čo znamená veriť digitálnemu podpisu?
  - veriť hašovacej funkcii,
  - veriť asymetrickej šifre,
  - veriť certifikátu podpisovateľa.
- Ako ho vytvárať/používať?
  - EU projekt:  
[https://joinup.ec.europa.eu/asset/sd-dss/asset\\_release/all](https://joinup.ec.europa.eu/asset/sd-dss/asset_release/all)
  - Lock It: (Peter Rybár, <http://lockitin.webnode.sk/>),
  - slovensko.sk: Aplikácia D.Signer/XAdES.

Treba si zohnať certifikát, alebo eID a čítačku.



# Zhnutie

- Čo znamená veriť digitálnemu podpisu?
  - veriť hašovacej funkcii,
  - veriť asymetrickej šifre,
  - veriť certifikátu podpisovateľa.
- Ako ho vytvárať/používať?
  - EU projekt:  
[https://joinup.ec.europa.eu/asset/sd-dss/asset\\_release/all](https://joinup.ec.europa.eu/asset/sd-dss/asset_release/all)
  - Lock It: (Peter Rybár, <http://lockitin.webnode.sk/>),
    - slovensko.sk: Aplikácia D.Signer/XAdES.

Treba si zohnať certifikát, alebo eID a čítačku.



# Zhnutie

- Čo znamená veriť digitálnemu podpisu?
  - veriť hašovacej funkcii,
  - veriť asymetrickej šifre,
  - veriť certifikátu podpisovateľa.
- Ako ho vytvárať/používať?
  - EU projekt:  
[https://joinup.ec.europa.eu/asset/sd-dss/asset\\_release/all](https://joinup.ec.europa.eu/asset/sd-dss/asset_release/all)
  - Lock It: (Peter Rybár, <http://lockitin.webnode.sk/>),
  - slovensko.sk: Aplikácia D.Signer/XAdES.

Treba si zohnať certifikát, alebo eID a čítačku.



# Ďakujem za pozornosť.

Prečo neboli vtipy?

***Three logicians walk into a bar.***

The barman asks “does everyone want a drink?”

VIA 9GAG.COM

*The first logician says, “I don’t know”.*

*The second logician says, “I don’t know”.*

*The third logician says, “Yes”.*

