EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

jihomoravský kraj

# SPISOVÁ A ARCHIVNÍ SLUŽBA

## Elektronické/digitální podpisy (certifikáty)

## Metodický list

Autor: Jan Kozák, Metodik: Mgr. Hana Hrádková

Recenzent: Ing. Peter Štubňa

Rok vydání: 2023

# Obsah

## Cíle

- Žák definuje pojem elektronicky podpis a digitální certifikát
- Žák rozlišuje jednotlivé úrovně elektronických podpisů a typy certifikátů
- Žák dokáže zacházet s elektronickým podpisem a uvědomuje si nutnost ochrany své identity

## Dovednosti

- Žák umí zacházet s digitálním certifikátem
- Žák správně interpretuje pojmy elektronických podpisů a digitálních certifikátů
- Žák zná možnosti využití elektronických podpisů a digitálních certifikátů

## Kontrolní otázky

- Co je to elektronický podpis?
- Jakým technologických prostředkem mohu dokument podepsat?
- Kdo může v České republice vydávat kvalifikované elektronické podpisy?
- Jaké základní typy digitálních certifikátů (dle jejich účelu) máme? Popište jejich typické použití.

## Pracovní prostředí

Úlohu lze realizovat s pomocí počítače s připojením na internet. Pro práci je nutné mít práva lokálního administrátora.

Pro práci budeme potřebovat následující:

- Počítač s přístupem na internet. V rámci studia využije stránky, kde jsou popsané příklady
    - https://docs.microsoft.com/en-us/powershell/module/pki/new-selfsignedcertificate?view=windowsserver2022-ps
    - https://docs.microsoft.com/cs-cz/azure/vpn-gateway/vpn-gateway-certificates-point-to-site

- Nástroje: Nástroje v rámci operačního systému Windows (certmgr.msc a PowerShell)
- Aplikace MS WORD, Adobe Reader DC, příkazový řádek (CMD), konzoli Microsoft Management Console

# 1 Průběh výuky

Otevřete internetový prohlížeč pro vyhledávání informací

1. Opakování z předchozí hodiny (asymetrická kryptografie, PKI - Public Key Infrastructure).
2. Výklad nové látky v rámci tématu elektronický podpis a digitální certifikát.
3. Zadání úlohy v rámci cvičení.
4. Prezentace výsledků žáky.
5. Shrnutí nových poznatků.

# 2 Podklady k výuce


# ZÁKLADNÍ POJMY

STŘEDNÍ ŠKOLA **INFORMATIKY, POŠTOVNICTVÍ A FINANČNICTVÍ** BRNO

***Certifikační autorita (zkratka CA)*** *- je v asymetrické kryptografii subjekt, který vydává digitální certifikáty (elektronicky podepsané veřejné šifrovací klíče), čímž usnadňuje využívání PKI (Public Key Infrastructure) tak, že svojí autoritou potvrzuje pravdivost údajů, které jsou ve volně dostupném veřejném klíči uvedeny. Na základě principu přenosu důvěry (viz níže) tak můžeme důvěřovat údajům uvedeným v digitálním certifikátu za předpokladu, že důvěřujeme samotné certifikační autoritě.*

https://cs.wikipedia.org/wiki/Certifika%C4%8Dn%C3%AD_autorita

## Typy certifikačních autorit

- **Certifikační autorita**
  - Služba která zajišťuje vydání certifikátu
  - Provozuje ji řada komerčních společností
  - Usnadňuje rozhodování o míře důvěry např. u webových stránek (důvěryhodná stránka, které věří daný prohlížeč)
  - Mohu si udělat vlastní = negarantuje ale vůbec nic
- **Kvalifikovaná certifikační autorita**
  - Definována zákonem o elektronickém podpisu č. 227/2000 Sb
  - Seznam veden u MVČR (http://www.mvcr.cz/clanek/prehled-udelenych-akreditaci.aspx)
    - I.CA www.ica.cz
    - Postsignum, www.postsignum.cz
    - eIdentity, www.eidentity.cz

# ZÁKLADNÍ POJMY

STŘEDNÍ ŠKOLA **INFORMATIKY, POŠTOVNICTVÍ A FINANČNICTVÍ** BRNO

***Digitální certifikát,*** *- vydává certifikační autorita, je v asymetrické kryptografii digitálně podepsaný veřejný šifrovací klíč. Uchovává se ve formátu X.509, který (kromě jiného) obsahuje informace o majiteli veřejného klíče a vydavateli certifikátu (tvůrci digitálního podpisu, tj. certifikační autoritě). Certifikáty jsou používány pro identifikaci protistrany při vytváření zabezpečeného spojení (HTTPS, VPN atp.). Na základě principu přenosu důvěry je možné důvěřovat neznámým certifikátům, které jsou podepsány důvěryhodnou certifikační autoritou.*

Zdroj: https://cs.wikipedia.org/wiki/Digit%C3%A1ln%C3%AD_certifik%C3%A1t

## Třídy certifikátů

- Class 1 – určena pro jednotlivce, pro e-mail
- Class 2 – určena pro organizace, kde je vyžadováno prokázání identity
- Class 3 – určena pro servery a digitální podpisy, kde je potřeba nezávislé potvrzení identity certifikační autoritou
- Class 4 – určena pro on-line obchodní transakce mezi společnostmi
- Class 5 – určena pro soukromé subjekty nebo vládní bezpečnost

# ZÁKLADNÍ POJMY

STŘEDNÍ ŠKOLA **INFORMATIKY, POŠTOVNICTVÍ A FINANČNICTVÍ** BRNO

***Další důležité pojmy, které je dobré znát v souvislosti s digitálním podpisem.***

***Pamatuj si!***

*Kvalifikovaný certifikát pro el. podpis nahrazuje je na stejné úrovni jako tvůj osobní podpis daného dokumentu. Je nutné jej tedy chránit. Nikdy se tedy do rukou cizí osoby nesní dostat jeho privátní část.*

Zdroj: https://cs.wikipedia.org/wiki/Digit%C3%A1ln%C3%AD_certifik%C3%A1t

- **Elektronická značka**
  - technicky totéž jako el. Podpis = digitální certifikát
  - rozdíl je ten, že certifikát byl vydán pro organizaci, která se jí prokazuje
- **Časové razítko**
  - technicky totéž jako el. podpis
  - pokud bylo vydáno kvalifikovanou certifikační autoritou, osvědčuje čas podpisu
- **Certifikát – veřejná část**
  - je to veřejný šifrovací klíč, vydaný certifikační autoritou
  - mohu poslat či dát komukoliv – neohrožuji tak své bezpečí
- **Certifikát – privátní část**
  - soukromý šifrovací klíč, který je "v páru" k veřejnému klíči
  - musí být chráněný (heslo, hw token) – nesmím jej předat nikomu
- **Komerční certifikát**
  - "běžný" certifikát vydaný certifikační autoritou
- **Kvalifikovaný certifikát**
  - certifikát vydaný akreditovaným poskytovatelem certifikačních služeb jako "kvalifikovaný" podle zákona o el. Podpisu
- **Kořenový certifikát (certifikační autority)**
  - otec všech certifikátů, vydaných certifikační autoritou

# OBSAH CERTIFIKÁTU

STŘEDNÍ ŠKOLA **INFORMATIKY, POŠTOVNICTVÍ A FINANČNICTVÍ** BRNO

***Obsah certifikátu*** *- Data v certifikátu jsou popsána jazykem ASN.1. Výhody ASN.1 spočívají v nezávislosti na počítačové platformě a dobré čitelnosti pro člověka. K přenosu klíče se používá binární podoba DER nebo textový formát PEM či CER (zakódování pomocí Base64), případně ještě formáty PKCS#7/P7B nebo PKCS#12/PFX. Mezi různými formáty je možný převod pomocí vhodného nástroje.*

## Položky v certifikátu

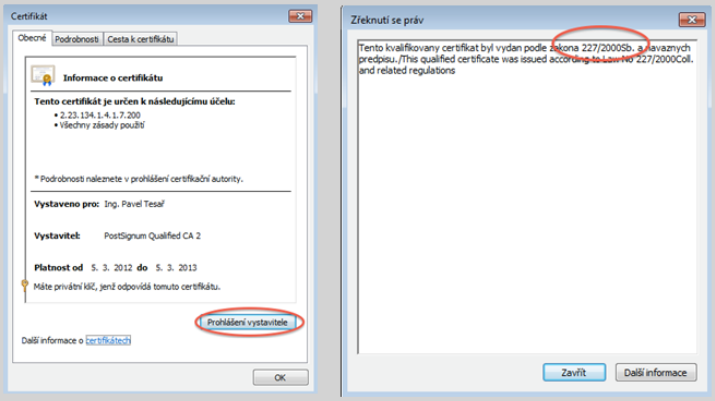
- Serial Number – (certifikáty mají pro lepší identifikaci vlastní sériové číslo, není to však nutnost)
- Subject – identifikační údaje majitele certifikátu
- Signature Algorithm – algoritmus použitý k vytvoření podpisu
- Signature – digitální podpis veřejného klíče vytvořený certifikační autoritou
- Issuer – identifikační údaje vydavatele certifikátu
- Valid-From – datum počátku platnosti certifikátu
- Valid-To – datum konce platnosti certifikátu; nejběžnější doba platnosti je jeden rok
- Key-Usage – účel veřejného klíče (šifrování, ověřování podpisů nebo obojí)
- Public Key – jeho bitová délka je závislá na druhu použitého šifrování
- Thumbprint Algorithm – algoritmus otisku certifikátu
- Thumbprint – vlastní otisk certifikátu sloužící k ověření neporušenosti certifikátu

# KONTROLNÍ OTÁZKA

STŘEDNÍ ŠKOLA **INFORMATIKY, POŠTOVNICTVÍ A FINANČNICTVÍ** BRNO

*Jak poznám kvalifikovaný certifikát?*

**Buď se podívám na prohlášení vystavitele v certifikátu:**





# KONTROLNÍ OTÁZKA

STŘEDNÍ ŠKOLA **INFORMATIKY, POŠTOVNICTVÍ A FINANČNICTVÍ** BRNO

*Jak poznám kvalifikovaný certifikát?*


**Nebo použiji webovou stránku https://tsl.gov.cz/:**

# SHRNUTÍ

*Elektronický podpis založený na certifikátu vydaném neakreditovanou certifikační autoritou nemá žádnou právní váhu.*

*Totéž platí pro elektronickou značku a časové razítko.*

**Uznávaný elektronický podpis = zaručený elektronický podpis založený na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb.**

**Je ekvivalentem podpisu osoby.**

**Obdobně hovoříme o uznávané elektronické značce a kvalifikovaném časovém razítku.**

**Jeho zneužití je trestné!!!!**

# INFORMAČNÍ ZDROJE

*Báječný svět elektronického podpisu*

*Elektronická kniha Jiřího Peterky, viz http://www.bajecnysvet.cz/*

*Naprosto všeobjímající a podrobný průvodce*

**Oficiální stránky Ministerstva vnitra**

**http://www.mvcr.cz/clanek/informace-k-pouzivani-elektronickeho-podpisu.aspx**

**Ověřování kvalifikovaných certifikátů**

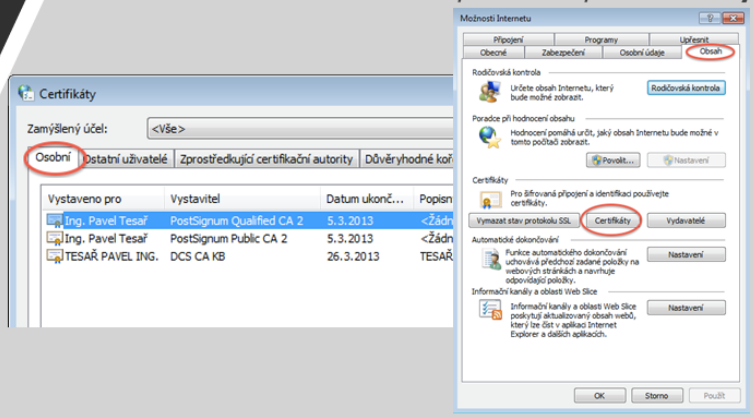
http://tsl.gov.cz/

# ULOŽENÍ CERTIFIKÁTŮ

STŘEDNÍ ŠKOLA **INFORMATIKY, POŠTOVNICTVÍ A FINANČNICTVÍ** BRNO

*Kde jsou na počítači s operačním systémem Windows uloženy certifikáty?*

**Odpověď: Ve Windows jsou obvykle v úložišti certifikátů, viz "Možnosti internetu" / Obsah / Certifikáty.**





# ULOŽENÍ CERTIFIKÁTŮ

STŘEDNÍ ŠKOLA **INFORMATIKY, POŠTOVNICTVÍ A FINANČNICTVÍ** BRNO

*Kde jsou na počítači s operačním systémem Windows uloženy certifikáty?*


**Ale mohou být i na čipové kartě nebo na USB tokenu, na advokátním průkazu, na elektronickém občanském průkazu…**


# POUŽITÍ CERTIFIKÁTŮ

STŘEDNÍ ŠKOLA **INFORMATIKY, POŠTOVNICTVÍ A FINANČNICTVÍ** BRNO

***Zopakujme si některé způsoby použití certifikátů.***

- **Serverový komerční (SSL) certifikát**
  - autentizuje server vůči uživateli (aby si uživatel mohl být jist, že je na správném serveru = ochrana proti podvržení web stránek)
  - šifruje komunikaci mezi serverem a klientem
- **Osobní komerční certifikát**
  - autentizuje uživatele vůči serveru (slouží k přihlášení uživatele k webové aplikaci – např. elektronické bankovnictví nebo do datové schránky)
  - lze využít např. pro šifrování dat na PC, šifrování emailu apod.
- **Osobní kvalifikovaný certifikát**
  - slouží k vytváření uznávaného elektronického podpisu
- **Certifikát pro podpis kódu**
  - Slouží k ověření výrobce daného software

# PRAKTICKÉ CVIČENÍ

STŘEDNÍ ŠKOLA **INFORMATIKY, POŠTOVNICTVÍ A FINANČNICTVÍ** BRNO

***Vytvoříme si certikát/y prostřednictvím Power Shell***

- Pro vytváření certifikátu použijeme nástroj od Microsoft Power Shell
- Jako vodítko nám poslouží stránky
  - https://docs.microsoft.com/en-us/powershell/module/pki/new-selfsignedcertificate?view=windowsserver2022-ps
  - https://docs.microsoft.com/cs-cz/azure/vpn-gateway/vpn-gateway-certificates-point-to-site

# PRAKTICKÉ CVIČENÍ

STŘEDNÍ ŠKOLA INFORMATIKY, POŠTOVNICTVÍ A FINANČNICTVÍ BRNO

***Vytvoříme si různé typy certifikátů a naučíme se s nimi pracovat. Pro tvorbu použijeme vzorové návody.***

- **Kořenový certifikát**
  - Slouží v rámci počítače k ověření klientských certifikátů.
  - Pokud není vystaven důvěryhodnou autoritou, tak je mu důvěřováno jen na zařízeních v nichž je importován.
- **Klientský certifikát**
  - Poslouží nám později pro digitální podpis dokumentu.
  - Je možné ho použít i pro další činnosti, u kterých je zapotřebí digitálního podpisu.

# PRAKTICKÉ CVIČENÍ

STŘEDNÍ ŠKOLA INFORMATIKY, POŠTOVNICTVÍ A FINANČNICTVÍ BRNO

***Tvorba kořenového certifikátu.***

Nutná podmínka pro kontrolu platnosti všech certifikátů, vydaných konkrétní certifikační autoritou.

- **Postup:**
  - **Vytvořím certifikát prostřednictvím PowerShell viz příklad**
  - **Ověřím jeho vytvoření prostřednictvím certmgr.msc**

# PRAKTICKÉ CVIČENÍ

STŘEDNÍ ŠKOLA INFORMATIKY, POŠTOVNICTVÍ A FINANČNICTVÍ BRNO

***Tvorba klientského certifikátu.***

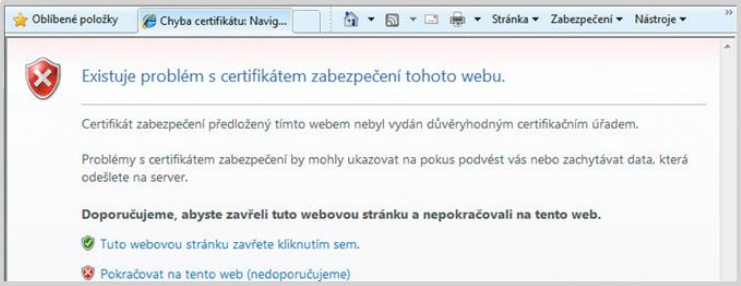
Certifikát vytvoření pro konkrétního klienta, může být použit pro podpis dokumentu, připojení pomocí VPN, ověření RDP atd.

- **Postup:**
  - **Vytvořím certifikát prostřednictvím PowerShell viz příklad**
  - **Ověřím jeho vytvoření prostřednictvím certmgr.msc**

# PRAKTICKÉ CVIČENÍ

STŘEDNÍ ŠKOLA INFORMATIKY, POŠTOVNICTVÍ A FINANČNICTVÍ BRNO

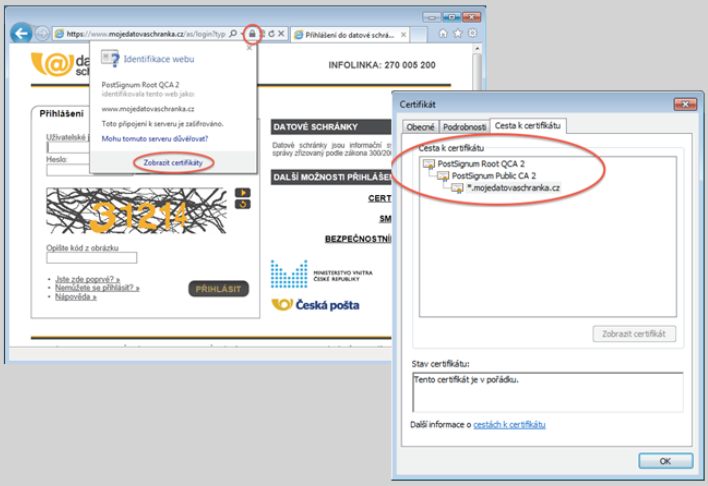
***Pokud nemám nainstalovaný kořenový certifikát, tak typicky můj webový server nebude pro klientskou stanici důvěryhodný***



# PRAKTICKÉ CVIČENÍ

STŘEDNÍ ŠKOLA **INFORMATIKY, POŠTOVNICTVÍ A FINANČNICTVÍ** BRNO

***Když mám kořenový certifikát, web je důvěryhodný, zobrazí se a můžu si zkontrolovat "zámeček".***

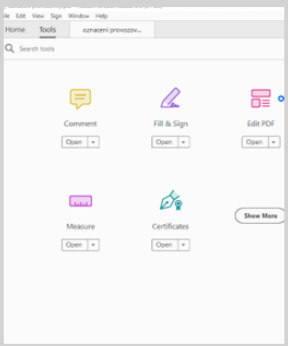



# PRAKTICKÉ CVIČENÍ

STŘEDNÍ ŠKOLA **INFORMATIKY, POŠTOVNICTVÍ A FINANČNICTVÍ** BRNO

***Podepisování PDF dokumentů (Adobe Acrobat)***

- Otevřu dokument v Acrobatu (verze 2022)
  - dokument musí být vytvořen tak, aby měl povolené podepisování
  - Klepnu na " Tools -> Certificates"
- pozn.:
  - povolení podepisování umožňuje plná verze Adobe Acrobat
  - podepisovat umí i Acrobat Reader DC

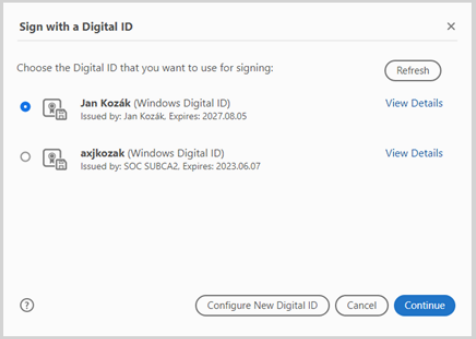


# PRAKTICKÉ CVIČENÍ

STŘEDNÍ ŠKOLA **INFORMATIKY, POŠTOVNICTVÍ A FINANČNICTVÍ** BRNO

***Podepisování PDF dokumentů (Adobe Acrobat)***

- ❑ Zvolím umístění v dokumentu
- ❑ Mohu vytvořit nový certifikát pomocí „Configure New Digital ID“
- ❑ Nebo vyberu certifikát

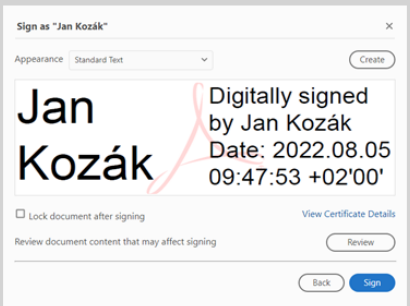



# PRAKTICKÉ CVIČENÍ

STŘEDNÍ ŠKOLA **INFORMATIKY, POŠTOVNICTVÍ A FINANČNICTVÍ** BRNO

***Podepisování PDF dokumentů (Adobe Acrobat)***

- ❑ Umístím podpis do rámečku na stránku
- ❑ Zvolím podepsat a uložím do nového dokumentu
- ❑ V Adobe mohu po opětovném otevření ověřit detaily podpisu

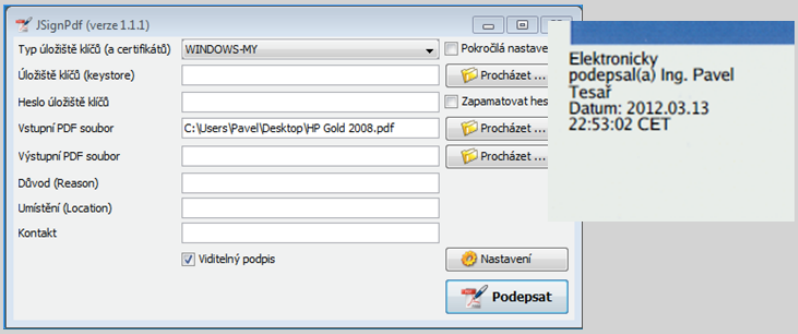


# PRAKTICKÉ CVIČENÍ

STŘEDNÍ ŠKOLA INFORMATIKY, POŠTOVNICTVÍ A FINANČNICTVÍ BRNO

***Podepisování PDF dokumentů (JSignPdf)***

- Zdarma dostupný program, viz http://jsignpdf.sourceforge.net/
  - Spustím program JSignPdf
  - Vyberu PDF soubor
  - Dám podepsat
  - Prohlédnu výsledek

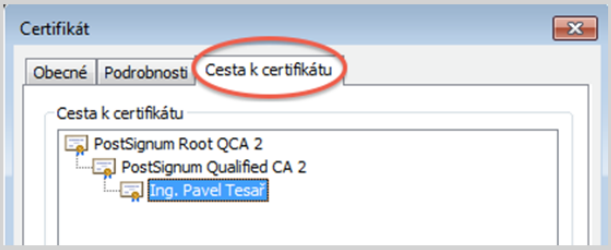



# PRAKTICKÉ CVIČENÍ

STŘEDNÍ ŠKOLA INFORMATIKY, POŠTOVNICTVÍ A FINANČNICTVÍ BRNO

***Jak poznám, že je elektronický podpis platný?***

- Provedu postupně:
  - ověření integrity dokumentu
  - ověření platnosti certifikátu k datu podpisu (bez časového razítka nelze)
  - ověření, zda certifikát nebyl zneplatněn (revokován)
- To celé opakuji pro každý certifikát na cestě



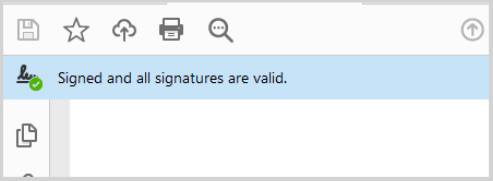
# PRAKTICKÉ CVIČENÍ

STŘEDNÍ ŠKOLA **INFORMATIKY, POŠTOVNICTVÍ A FINANČNICTVÍ** BRNO

***Ověřování elektronického podpisu v Adobe Acrobat.***

- Adobe Acrobat nabízí uživatelům podporu při ověření stavu podpisů.
- Prohlásí tedy za platné i podpisy, které jsou založeny na komerčním certifikátu.

Neumí nicméně automatizovaně rozpoznat uznávané elektronické podpisy.



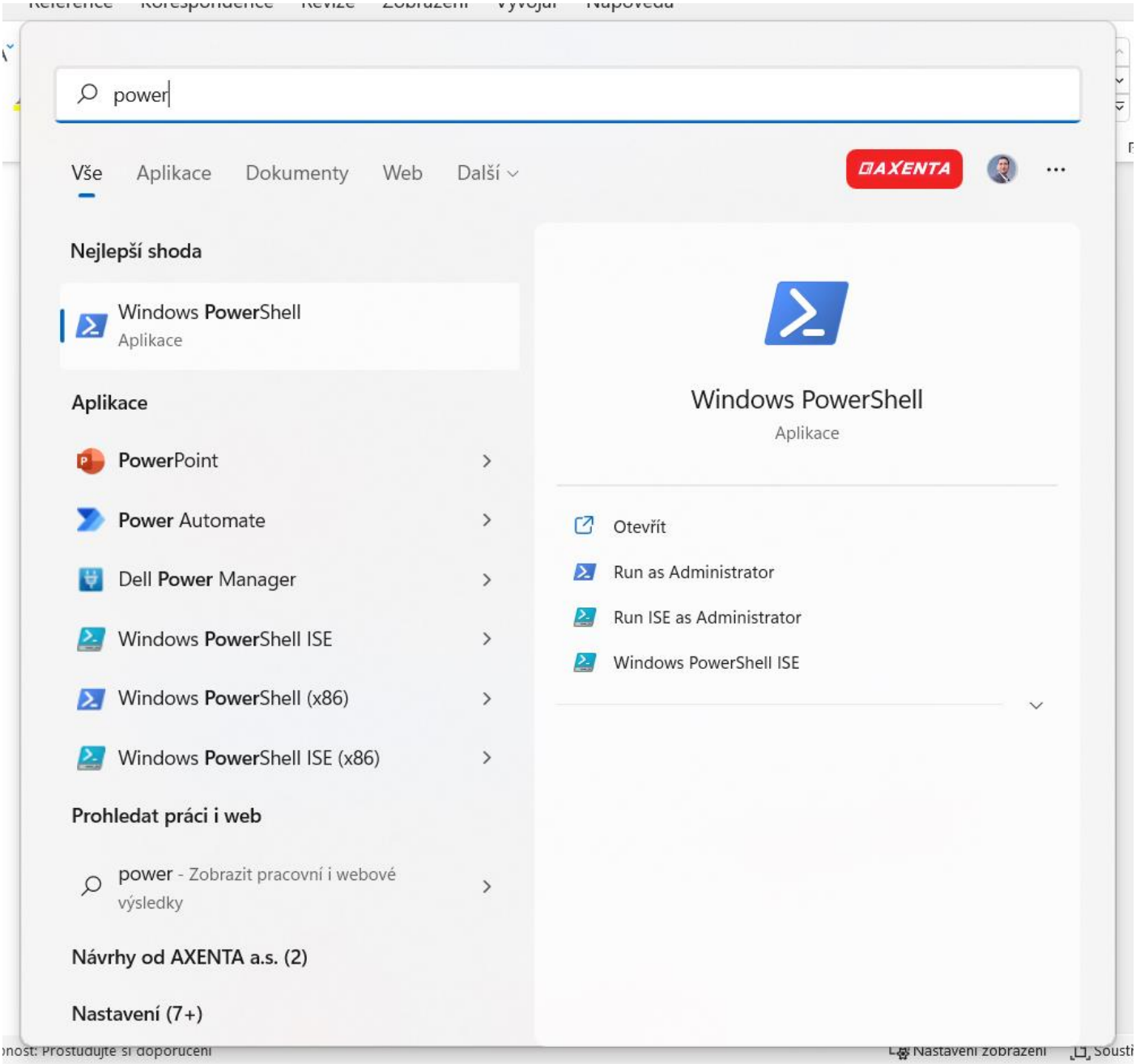

## Děkuji za pozornost

# 3 Zadání

## 3.1 Vytvořte root certifikát

Tvorba root certifikátů.

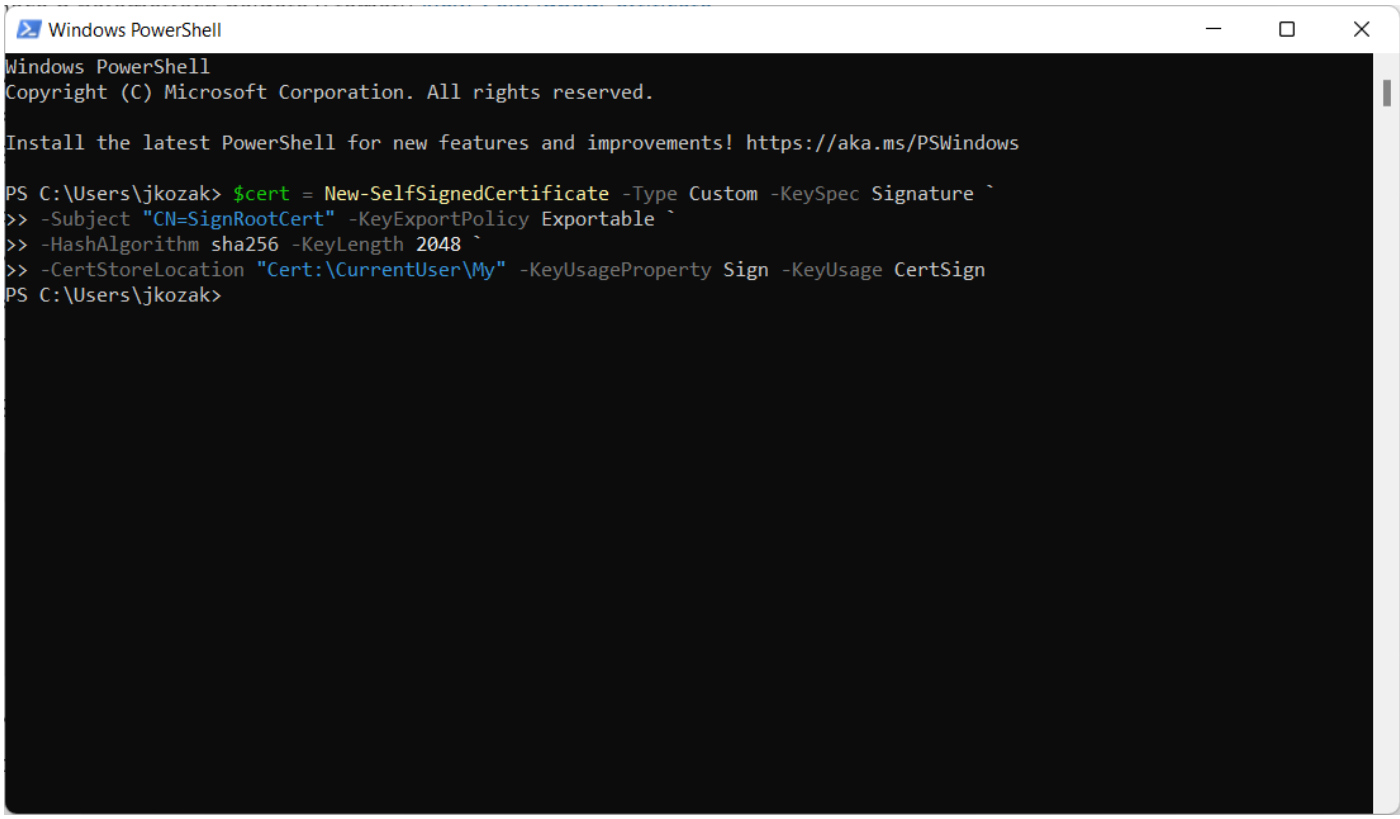
a) Pomocí tlačítka Win a zapsáním PowerShell vyhledejte tuto aplikace a spušťtě



b) Zapiště do PowerShell následující přikaz

```
$cert = New-SelfSignedCertificate -Type Custom -KeySpec Signature `
-Subject "CN=SignRootCert" -KeyExportPolicy Exportable `
-HashAlgorithm sha256 -KeyLength 2048 `
-CertStoreLocation "Cert:\CurrentUser\My" -KeyUsageProperty Sign -KeyUsage CertSign
```

c) Žák si pojmenuje root cetifikát libovolně.

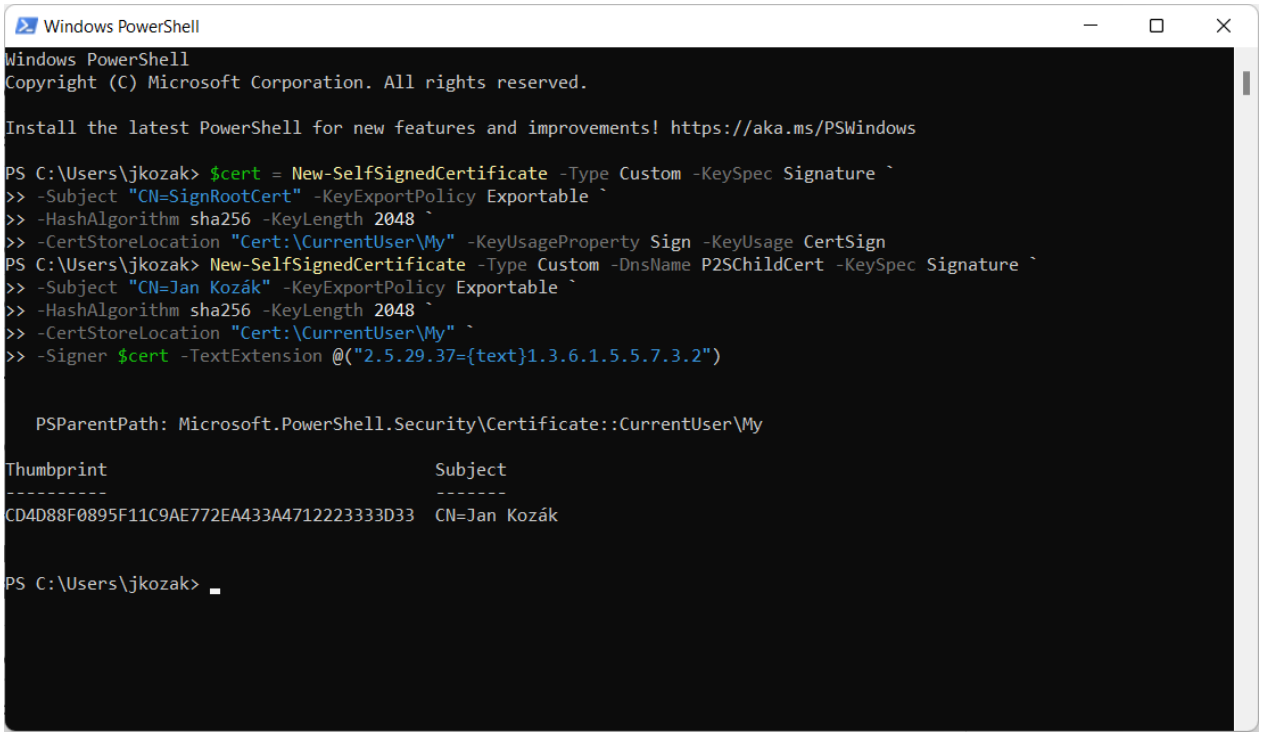



d) Nezavírejte PowerShell

## 3.2 Vytvořte klientský certifikát (osobní)

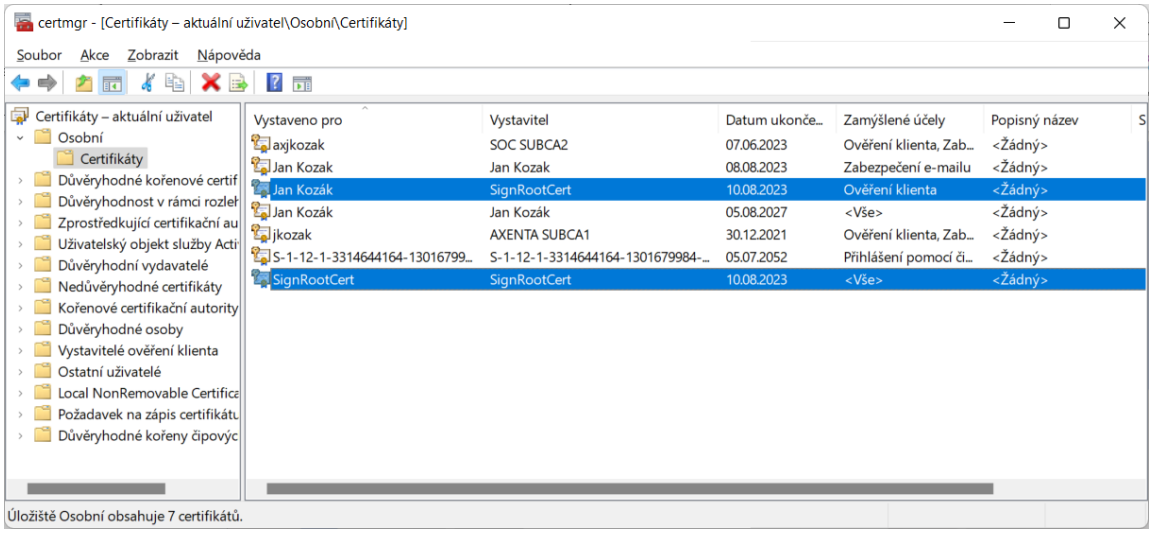
a) V rámci již otevřené konzole pokračujte tvorbou klientského certifikátu

```
New-SelfSignedCertificate -Type Custom -DnsName P2SChildCert -KeySpec Signature `
-Subject "CN=Jan Kozák" -KeyExportPolicy Exportable `
-HashAlgorithm sha256 -KeyLength 2048 `
-CertStoreLocation "Cert:\CurrentUser\My" `
-Signer $cert -TextExtension @("2.5.29.37={text}1.3.6.1.5.5.7.3.2")
```

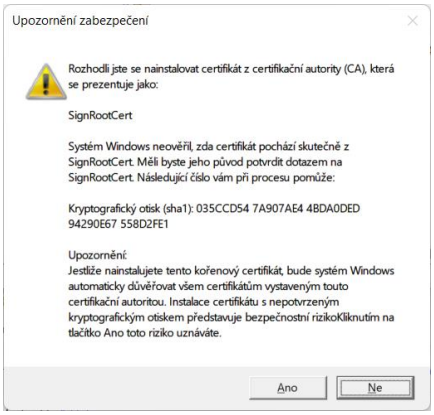



b) Ověřte, že je certifikát správně vygenerovaný prostřednictvím cert.mgr.

   a. Stiskněte WIN+R
   b. Napište certmgr.msc
   c. Zkontrolujte v části osobí vytvořené certifikáty




c) Klientský certifikát nyní není důvěryhodný, přesuňte ho do Důvěryhodné kořenové certifikační autority. Přesunutí se provede např. přetažením myší.

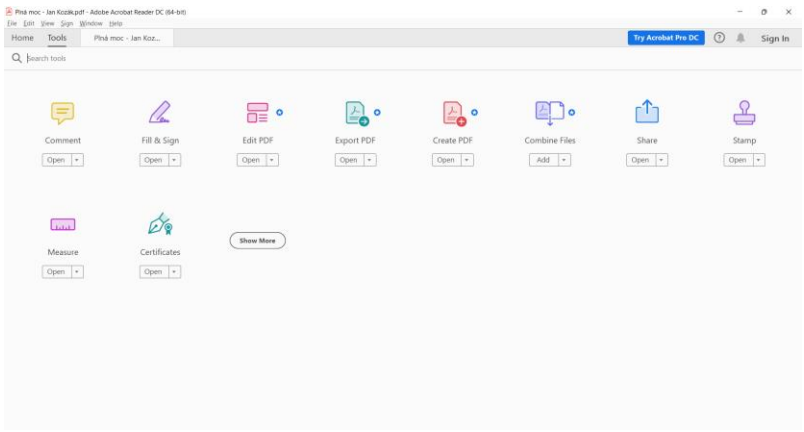



d) Ověříme, zda je certifikát správně uložen a následně se podíváme, zda je klientský certifikát již důvěryhodný.

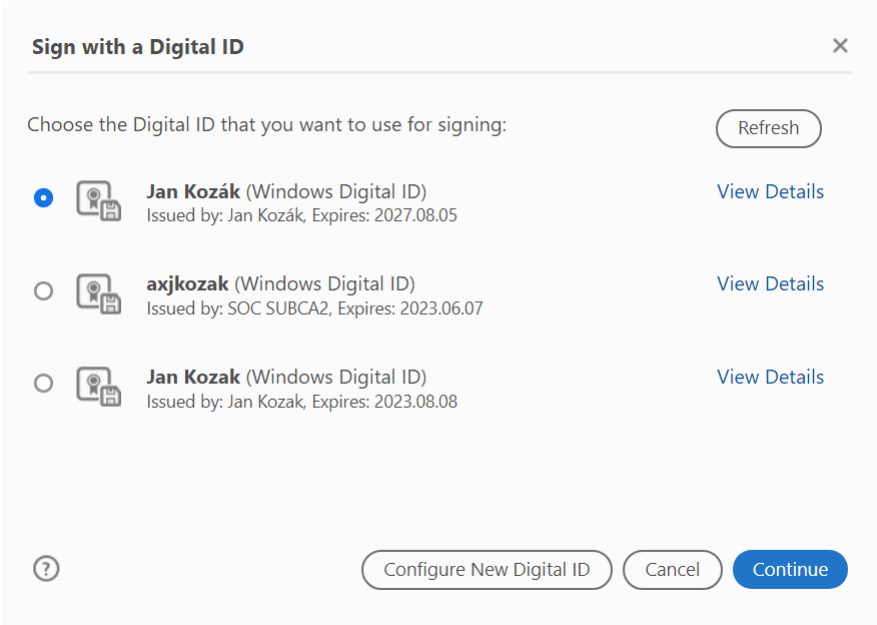

## 3.3 Podepište dokument osobní certifikátem

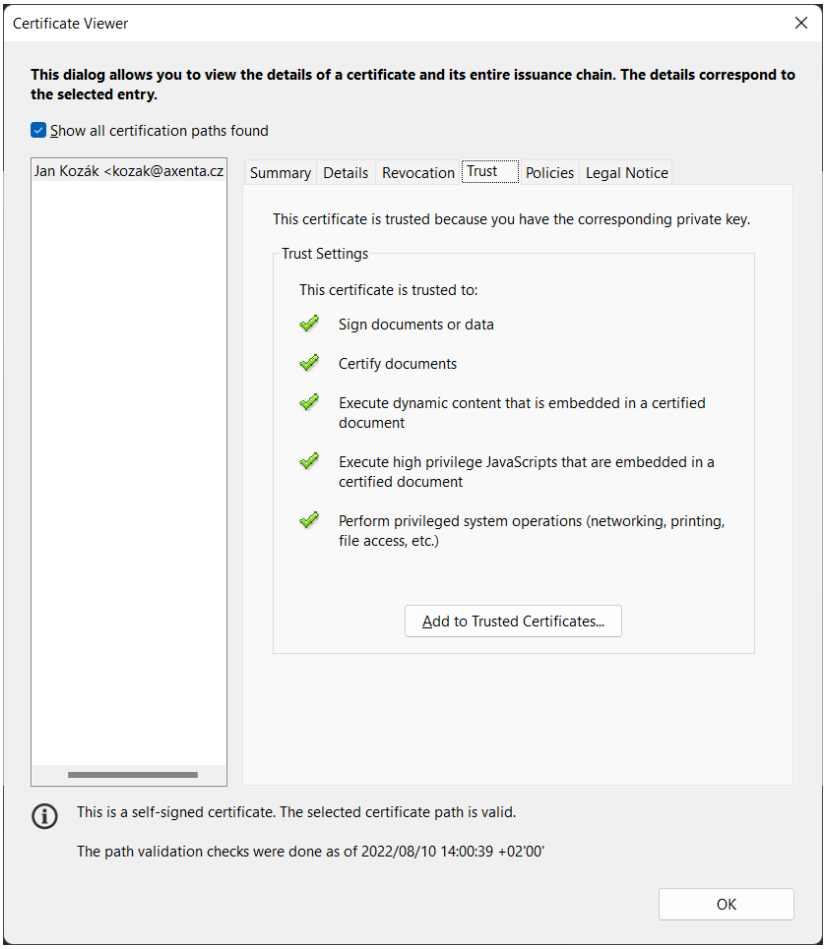
Máme připraveny certifikáty pro podpis dokumentu.

a) Student si vytvoří ve Wordu dokument, např. plnou moc. Následně ji uloží ve formátu PDF do složky kterou si vytvořil
b) Stáhneme nebo již využijeme již staženy Acrobat Reader DC a PDF dokument otevřeme. Byly v tomto listě použita verze 2022. Postup se můře lišit ve straších verzích.
c) Zvolíme TOOLS a Certificates
d) Následně klikněte na Digitally Sign a vyberte místo podpisu

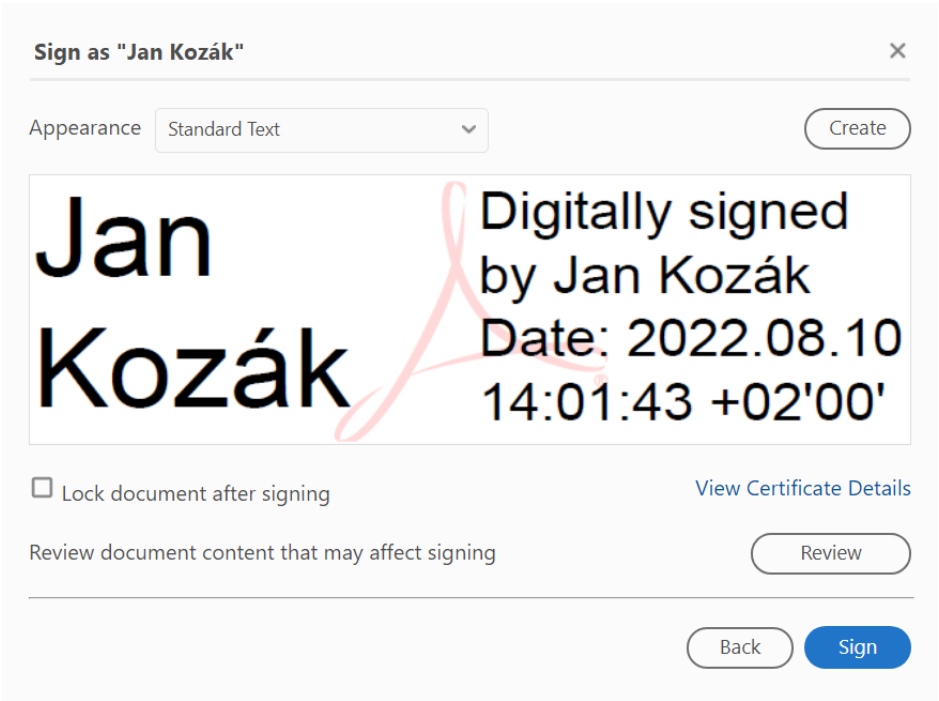



e) Vyberte vytvořený certifikát ve View Details můžete zkontrolovat, zda je certifikátu opravdu důvěřováno.






f) V náhledu vidíte, jak bude podpis vypadat a dokument rovnou uložte i s podpisem




g) Můžete ukončit všechny aplikace

## 3.4 Popište typická použití certifikátů a na internetu najděte příklady

Žák popíše jednotlivé příklady použití. Jeden byl procvičen v rámci listu a to podpis dokumentu.

Žák zde využije znalosti, které získal při výkladu.

Typické použití.

a) Digitální podpis dokumentu
    a. Může ukázat na vypracovaném dokumentu
b) Zabezpečení e-mail komunikace
    a. Může ukázat na podepsaném e-mailu, pokud takový má
c) Ověření webových stránek a jejich zabezpečení = https stránky
    a. Může ukázat na libovolné https stránce
d) Podpis kódu v rámci software
    a. Může ukázat např. na Adobe Reader, který má soubory podepsané

# Seznam použitých zdrojů


- https://docs.microsoft.com/en-us/powershell/module/pki/new-selfsignedcertificate?view=windowsserver2022-ps
- https://docs.microsoft.com/cs-cz/azure/vpn-gateway/vpn-gateway-certificates-point-to-site