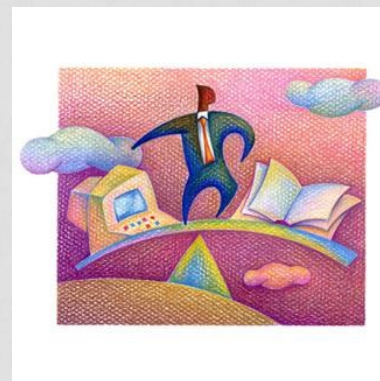




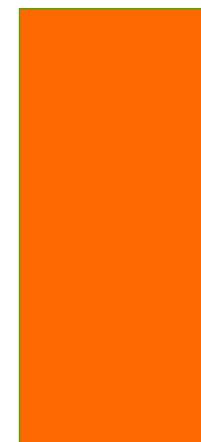
VY_32_INOVACE_IKTO2_1760_PCH

VÝUKOVÝ MATERIÁL V RÁMCI PROJEKTU OPVK 1.5 PENÍZE STŘEDNÍM ŠKOLÁM

ČÍSLO PROJEKTU:	CZ.1.07/1.5.00/34.0883
NÁZEV PROJEKTU:	ROZVOJ VZDĚLANOSTI
ČÍSLO ŠABLONY:	III/2
DATUM VYTVOŘENÍ:	5. 6. 2013
AUTOR:	MGR. LENKA PCHÁLKOVÁ
URČENO PRO PŘEDMĚT:	INFORMAČNÍ A KOMUNIKAČNÍ TECHNOLOGIE
TEMATICKÁ OBLAST:	INFORMAČNÍ ZDROJE, ELEKTRONICKÁ KOMUNIKACE, KOMUNIKAČNÍ A PŘENOSOVÉ MOŽNOSTI INTERNETU
OBOR VZDĚLÁNÍ:	OBCHODNÍK (66-41-L/01) 2. ROČNÍK
NÁZEV VÝUKOVÉHO MATERIÁLU:	ZABEZPEČENÍ A ŠIFROVÁNÍ
POPIS VYUŽITÍ:	ŽÁK PRACUJE S POJMY DIGITÁLNÍ CERTIFIKÁT, CERTIFIKAČNÍ AUTORITA, ZABEZPEČENÝ PROTOKOL. VYHLEDÁ CERTIFIKÁTY VE SVÉM POČÍTAČI. OVĚŘÍ ZAŠIFROVANÉ A NEZAŠIFROVANÉ STRÁNKY.
ČAS:	13 MINUT



ZABEZPEČENÍ A ŠIFROVÁNÍ



Zabezpečení a šifrování

Cenná data

Osobní údaje (rodné číslo, adresy)

Zdravotní stav

Majetkové poměry

Info o vzdělání

Info o platech

Marketingové strategie

Vojenské informace

Firemní strategie a plány

... doplňte vlastní zkušenost

Zabezpečení a šifrování

Šifrování je spolehlivá metoda ochrany dat.

S protokolem **https://** (Hyper Text Transfer Protocol Secure) jsme se potkali v prezentaci internetové bankovnictví.

Pro práci se stránkami musíte mít nainstalovaný a odsouhlasený digitální certifikát.

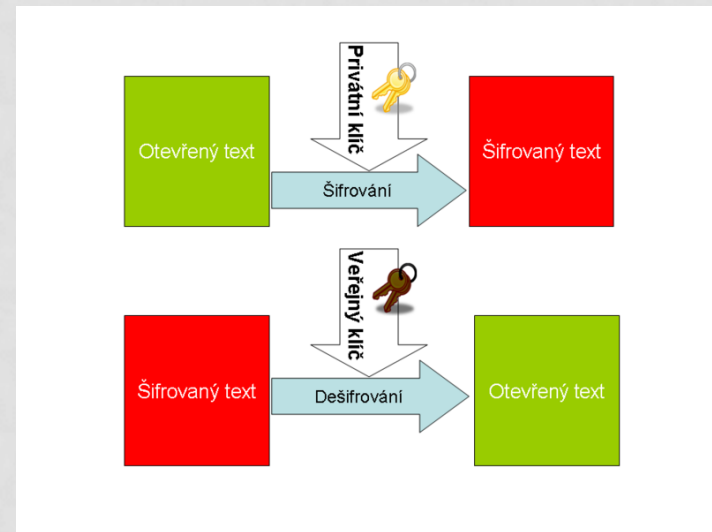
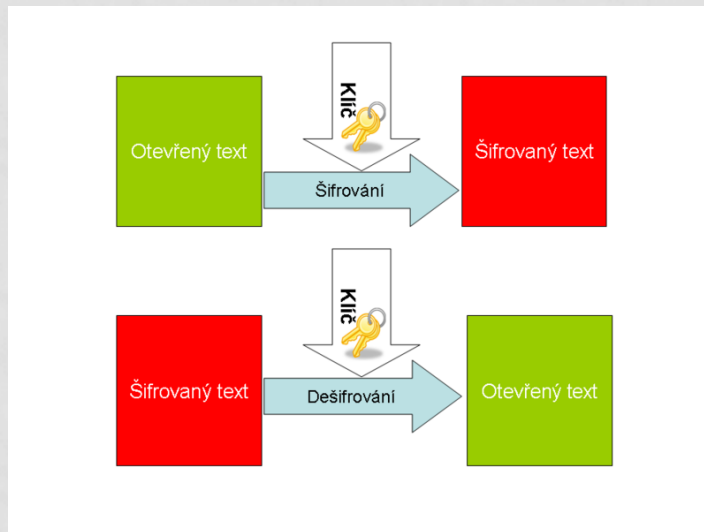
Přenos dat mezi prohlížečem a serverem bude probíhat bezpečně.



Digitální certifikát

Digitálně podepsaný veřejný klíč s jehož pomocí se uskutečňuje vzájemná kryptovaná komunikace serveru a www prohlížeče.

Schéma symetrické a asymetrické kryptografie



Certifikační autorita (CA)

Subjekt vydávající digitální certifikáty (elektronicky podepsané šifrovací klíče).

Potvrzuje, že server, který disponuje daným certifikátem, je skutečně tím, za který se vydává. (*Pravost je popsána certifikační autoritou*).

Aby prohlížeč mohl ověřit pravost tohoto podpisu, musí mít www prohlížeč tuto certifikační autoritu uloženu v seznamu autorit.

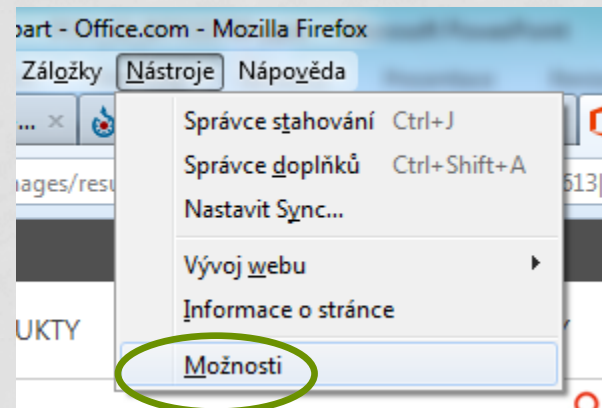
Instalace certifikátu

Je-li stránka zabezpečená protokolem https, pak se po zadání zobrazí hlášení o vstupu do zabezpečené zóny.

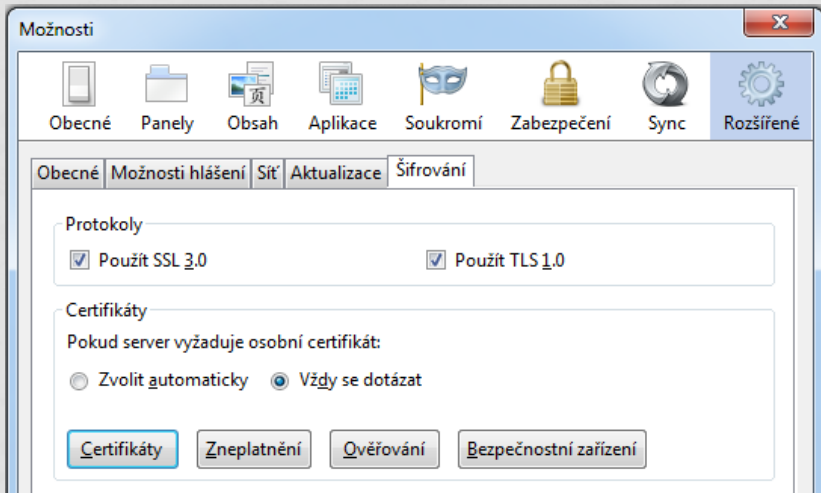
Bezpečnostní certifikát si uživatel nainstaluje do svého prohlížeče.

Prohlédněte si certifikáty nainstalované ve vašem PC v úložišti certifikátů.

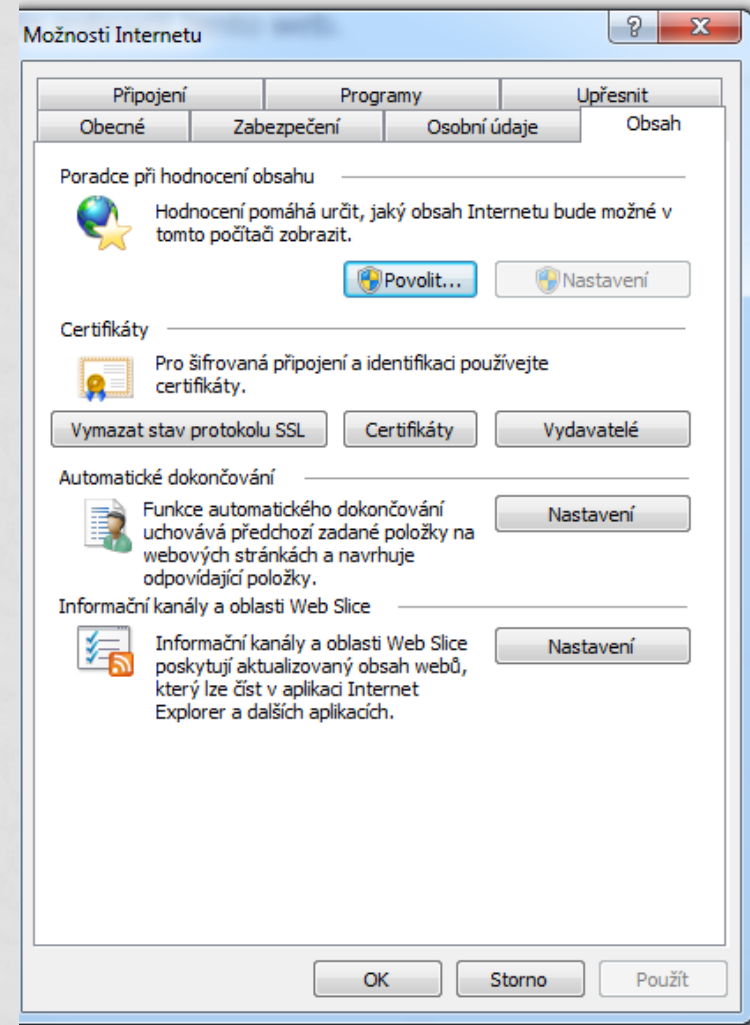
Budeme hledat Možnosti v Nástrojích prohlížeče.
Např.



Úložiště certifikátů



V této části můžeme certifikáty editovat.



Ukázka nezašifrovaného spojení

The screenshot shows a browser window with the title "Informace o stránce - http://www.ceskatelevize.cz/ct24/media-it/213315-televizni-digitalizac...". The browser's address bar and tabs are visible. The main content area is divided into several sections, with two sections highlighted by green ovals:

- Identita webového serveru** (Server Identity):
 - Webový server: **www.ceskatelevize.cz**
 - Vlastník: **Tato stránka neposkytuje informace o vlastníkovi**
 - Ověřovatel: **Není nastaven**
- Technické detaily** (Technical Details):
 - Spojení není zašifrováno**
 - Webový server **www.ceskatelevize.cz** nepodporuje šifrování pro zobrazenou stránku.
 - Informace odeslané do Internetu bez zašifrování mohou být při přenosu zneužity cizími osobami.

Other visible sections include "Soukromí a historie" (Privacy and History) with statistics for server visits and cookies, and a navigation bar with icons for "Obecné", "Média", "Povolení", and "Bezpečnost".

Ukázka zašifrovaného spojení

Informace o stránce - https://www.mojedatovaschranka.cz/as/login?uri=https%3a%2f%2fwww.moje...

Obecné Povolení **Bezpečnost**

Identita webového serveru

Webový server: **www.mojedatovaschranka.cz**
Vlastník: **Ministerstvo vnitra**
Ověřovatel: **GeoTrust Inc**

Zobrazit certifikát

Soukromí a historie

Navštívil jsem už někdy tento server?	Ne	
Má tento server uložené cookies na mém počítači?	Ano	Zobrazit cookies
Mám pro tento server uložená hesla?	Ne	Zobrazit uložená hesla

Technické detaily

Spojení zašifrováno: vysoký stupeň bezpečnosti (AES-256, klíč 256 bitů)
Zobrazená stránka byla před přenosem přes Internet zašifrována.
Šifrování velmi ztěžuje neoprávněným osobám sledovat informace mezi počítači. Je proto velmi nepravděpodobné, že by někdo dokázal přečíst tuto stránku při průchodu sítí.

Použitá literatura a internetové zdroje

- NAVRÁTIL, Pavel. *S počítačem nejen k maturitě - 1. díl*. 7. vyd. Computer Media, spol. s r.o., 2009. ISBN 978-80-7402-020-9.
- NAVRÁTIL, Pavel. *S počítačem nejen k maturitě*. 7. vyd. Kralice na Hané: Computer Media, 2009, 176 s. ISBN 978-80-7402-021-6.
- ROUBAL, Pavel. *Informatika a výpočetní technika pro střední školy: teoretická učebnice*. Vyd. 1. Brno: Computer Press, 2010, 103 s. ISBN 978-80-251-3228-9.
- Kliparty viz Galerie médií Microsoft PowerPoint.
- ROUBAL, Pavel. *Informatika a výpočetní technika pro střední školy: teoretická učebnice*. Vyd. 1. Brno: Computer Press, 2010, 103 s. ISBN 978-80-251-3228-9.
- {{Information | Description= {{cs | Schéma asymetrické kryptografie.}} {{en | Public-key cryptography scheme.}} | Source= *self work *Transferred from [http://cs.wikipedia.org cs.wikipedia]; Transfer was stated to be made by [User:sevela.p.](#) | Date=2007-12-1 http://upload.wikimedia.org/wikipedia/commons/6/60/Asymetrick%C3%A1_kryptografie.png {{Information | Description= {{cs | Princip symetrické kryptografie v češtině.}} {{en | Symmetric-key algorithm axiom in Czech.}} | Source= *self work *Transferred from [http://cs.wikipedia.org cs.wikipedia]; Transfer was stated to be made by [[User:sevela. http://commons.wikimedia.org/wiki/File:Symetrick%C3%A1_%C5%A1ifra.png?uselang=cs