

Protože dbáme bezpečnosti při elektronické komunikaci, zabezpečujeme mnoho školních webových služeb proti odposlechu pomocí zabezpečeného připojení (https). Jedná se o tyto stránky (sekce pro učitele), školní e-mail, e-learning moodle, žákovská knížka Bakaláři, imap, smtp a další . Od 1. ledna 2016 jsme přešli na využívání nové veřejné certifikační autority [Let's Encrypt](#) [1], která podepisuje téměř všechny naše certifikáty.

Starý návod na uznání naší vlastní školní certifikační autority:

K vydávání certifikátů těchto služeb provozujeme **vlastní certifikační autoritu AG** (AG_CA). Doporučujeme všem uživatelům, aby si tuto certifikační autoritu přidali jako důvěryhodnou kořenovou certifikační autoritu - jinak prohlížeč webu varuje před neznámým certifikátem a nedoporučuje pokračování. Po uznání naší certifikační autority prohlížeč dokáže ověřit spojení s AG a to je zabezpečené podobně dobře, jako třeba komunikace s bankou.

Postup, jak uznat naši certifikační autoritu:

Postup se liší v různých prohlížečích:

- Ve Firefoxu je to nejsnazší: kliknete na přílohu tohoto článku [scertifikátem](#) [2] a zaškrtnete: Důvěřovat pro ověření webových stránek.
- Pro Internet Explorer a Chrome ve Windows je nutné stažený certifikát otevřít a importovat do úložiště certifikátů. Přitom vybrat skupinu Důvěryhodné kořenové certifikační autority.
- Chrome v Linuxu vyžaduje příkaz:

```
certutil -d sql:$HOME/.pki/nssdb -A -t "C,," -n AG_CA -i ca.crt
```

Kontrolní součty certifikátu naší certifikační autority:

- fingerprint SHA-256:
B2:54:30:3D:1C:34:75:17:B3:80:D7:12:9C:96:0E:36:89:98:72:97:72:6D:AC:86:32:44:DE:1D:03:08:DE:BF
- fingerprint SHA-1: 4B:64:E2:87:6A:AD:57:2F:81:3A:51:BF:89:4D:14:48:92:95:CE:B1

Příloha:

[Certifikát certifikační autority AG](#) [2]

« Zpět

URL zdroje: <https://www.arcig.cz/certifikacni-autorita>

Odkazy

[1] <https://letsencrypt.org>

[2] <https://www.arcig.cz/sites/default/files/ca.crt>