

# Elektronický podpis

---

# Co to je?

---

V podstatě digitální ekvivalent fyzického podpisu.

Využití dat, které jsou jasně spojeny s jinými daty, nebo osobou k jasnému ověření totožnosti dané osoby.

Zajišťují autenticitu, integritu a nepopiratelnost daného dokumentu.

# Jak to funguje?

---

Používá buď metodu Asymetrické kryptografie nebo Symetrické šifry.

Asymetrické kryptografie – Časově náročnější, má však lehce bezpečnější výsledek.

Symetrické šifry – Výrazně rychlejší, negeneruje však zcela důvěryhodné podpisy

# Kdo ho vydává?

---

Obecně vydavatele dělíme na Akreditované, veřejné, a soukromé Certifikační Autority.

Akreditované CA – Vyžadovány pro komunikaci se státní správou, velmi vysoká bezpečnost využití, musí plnit určité, zákonem dané podmínky. V ČR je to První certifikační autorita (<https://www.ica.cz/>) Česká pošta ([https://www.postsignum.cz/certifikat\\_online.html](https://www.postsignum.cz/certifikat_online.html)) a Eidentity (<https://www.eidentity.cz/>)

Veřejné CA – Nejsou akreditované, ale stále nabízí své služby veřejnosti

Soukromé CA – Z pravidla zařizované v rámci samostatných organizací, levnější pro provozovatele, z pravidla nedostupné široké veřejnosti.

# Kvalifikovaný vs komerční

---

Kvalifikovaný certifikát – Slouží výhradně k elektronickému podepisování, komunikace se státními subjekty a pojišťovnami, bezpečnost a důvěryhodnost je kontrolována úřady.

Komerční certifikáty – slouží převážně k bezpečné komunikaci a přihlašování, nejsou automaticky uznány při komunikaci se státní správou, ze strany zákona na ně nejsou kladeny požadavky, jejich důvěryhodnost je založena na souhlasu dvou komunikujících stran.

# Zdroje:

---

Budiš, Petr., & Štedroň, Bohumír. (2008) *Elektronická komunikace*. Magnet Press Slovakia.

Digitální podpis s.r.o. (n.d.) *Jaký je rozdíl mezi kvalifikovaným a komerčním certifikátem?*. <https://www.digitalni-podpis.cz/rozdil-mezi-komercnim-a-kvalifikovanim-certifikatem/>

Ministerstvo vnitra české republiky. (n.d.). *Přehled kvalifikovaných poskytovatelů certifikačních služeb a jejich kvalifikovaných služeb*. <https://web.archive.org/web/20090714125750/http://www.mvcr.cz/clanek/prehled-kvalifikovanych-poskytovatelu-certifikacnich-sluzeb-a-jejich-kvalifikovanych-sluzeb.aspx> (archivováno 2021).

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (2014) <https://eur-lex.europa.eu/eli/reg/2014/910/oj>

Zákon č. 297/2016 Sb. Zákon o službách vytvářejících důvěru pro elektronické transakce (2016) <https://www.zakonyprolidi.cz/cs/2016-297/zneni-20230401>