Co je public key

Poslední aktualizace 5 června, 2026

Public key (veřejný klíč) je část kryptografického páru klíčů, který se používá pro šifrování dat a ověřování identity.

Patří do tzv. asymetrické kryptografie – vždy existuje dvojice klíčů – veřejný a soukromý. Veřejný klíč můžete bezpečně sdílet, zatímco soukromý klíč musí zůstat tajný.

Jak veřejný klíč funguje

Veřejný klíč se používá společně se soukromým klíčem, ale každý z nich má jinou roli.

Zjednodušeně:

- veřejný klíč slouží k šifrování dat
- soukromý klíč slouží k jejich dešifrování

> *To znamená, že pokud někdo zašifruje zprávu vaším veřejným klíčem, přečíst ji můžete pouze vy – pomocí svého soukromého klíče.*

Veřejný klíč a ověřování identity

Veřejný klíč se nepoužívá jen pro šifrování, ale i pro ověřování.

Například při digitálním podpisu:

- zpráva se „podepíše“ soukromým klíčem
- ostatní ověří podpis pomocí veřejného klíče

Díky tomu lze ověřit, že zpráva skutečně pochází od daného odesílatele.

Proč je veřejný klíč důležitý

Veřejný klíč umožňuje bezpečnou komunikaci bez nutnosti sdílet tajné informace předem.

To je zásadní rozdíl oproti starším metodám šifrování, kde bylo nutné sdílet jedno společné

heslo.

Díky asymetrické kryptografii:

- můžete bezpečně komunikovat i s neznámým protějškem
- není nutné předem sdílet tajný klíč
- lze ověřit identitu odesílatele