Co je privátní klíč

Poslední aktualizace 1 června, 2026

Privátní klíč (private key) je tajný kryptografický klíč, který se používá k dešifrování dat nebo k vytváření digitálního podpisu.

> *Je součástí dvojice klíčů v asymetrické kryptografii. Zatímco veřejný klíč lze sdílet, privátní klíč musí zůstat uložený v bezpečí – kdokoliv by se k němu dostal, může se vydávat za jeho vlastníka.*

Jak privátní klíč funguje v praxi

Privátní klíč se používá vždy společně s veřejným klíčem. Každý z nich má jinou roli, ale fungují jako propojený pár.

V praxi se používá dvěma způsoby:

- pokud někdo zašifruje data vaším veřejným klíčem, dešifrovat je můžete jen vy pomocí privátního klíče
- pokud data „podepíšete“ svým privátním klíčem, ostatní mohou pomocí veřejného klíče ověřit, že jste je skutečně vytvořili

Při navazování HTTPS spojení server používá svůj privátní klíč k prokázání identity. Prohlížeč si tak ověří, že komunikuje se správným serverem.

Kde se privátní klíč používá

Privátní klíče jsou základní součástí zabezpečení komunikace i přístupu k systémům.

Typické použití:

- HTTPS a SSL/TLS certifikáty
- přihlašování pomocí SSH klíčů
- digitální podpisy dokumentů
- šifrování komunikace mezi systémy

Na serveru je privátní klíč uložený lokálně a používá se při každém navázání

zabezpečeného spojení.

Co se stane, když privátní klíč unikne

Bezpečnost privátního klíče je zásadní. Pokud ho někdo získá, může se vydávat za jeho vlastníka.

V praxi to například znamená, že:

- útočník může dešifrovat komunikaci
- může se vydávat za server nebo uživatele
- může podepisovat data jménem vlastníka

> *Únik privátního klíče k SSL certifikátu znamená, že útočník může vytvořit server, který bude pro uživatele vypadat jako legitimní.*

Jak privátní klíč chránit

Privátní klíč by měl být vždy uložený tak, aby k němu měl přístup pouze oprávněný uživatel nebo systém.

Základní pravidla:

- nikdy ho nesdílet ani neposílat
- ukládat ho šifrovaně nebo chráněný heslem
- omezit přístupová práva na minimum

Na serveru by měl být přístup ke klíči omezený jen na konkrétní proces, který ho vyžaduje.