

Jak zajistit bezpečnou komunikaci v digitálním prostředí? Odpovědí je PKI

24.1.2024 - Mariana Pohlová | PROTEXT

Díky šifrování a ověřování, které PKI umožňuje, je zajištěna důvěryhodná a bezpečná online komunikace. Pro organizace může využívání PKI znamenat rozdíl mezi tím, že se vetřelec dostane do sítě prostřednictvím připojeného zařízení, a tím, že se potenciálně nebezpečná hrozba udrží podstatně dále.

Ke klíčovým komponentům PKI patří:

PKI funguje na principu asymetrické kryptografie, kdy každý účastník má dva klíče: veřejný a soukromý. Veřejný klíč je dostupný komukoli, kdo o něj požádá, a slouží k zašifrování zprávy, kterou někdo pošle příjemci. Soukromý klíč je tajný a slouží k dešifrování zprávy po jejím přijetí. Klíče jsou propojeny složitým matematickým vztahem, který je těžké odvodit běžnými metodami.

Každé entitě, která chce komunikovat v rámci PKI, jsou přiřazeny certifikáty, tedy dokumenty, které fungují jako digitální pasy. Vydává je certifikační autorita. Certifikáty potvrzují, že osoba nebo zařízení, se kterým chcete komunikovat, je skutečně tím, za koho se vydává. Platnost certifikátu lze ověřit pomocí systému, který kontroluje, zda je pravý, nebo ne.

Jak funguje TeskaLabs SeaCat PKI?

Vlastní řešení PKI v podobě SeaCat PKI nabízí i česká technologická společnost TeskaLabs, zabývající se vývojem nástrojů kybernetické bezpečnosti.

SeaCat PKI je software pro centrální systém správy klíčů (KMS) a systém správy certifikátů (CMS), který usnadňuje bezpečný elektronický přenos informací. Používá se pro činnosti, které vyžadují prokázání totožnosti stran zapojených do komunikace

a ověření platnosti přenášených informací. Tato infrastruktura zajišťuje vydávání certifikátů pro zařízení od fáze jejich výroby, přes komunikaci mezi zařízeními až po ukončení životnosti.

SeaCat PKI charakterizuje silné zabezpečení, protože specialisté na kyberbezpečnost TeskaLabs průběžně vybírají kryptografické algoritmy, které jsou všeobecně uznávány jako nejsilnější. Jde o moderní mikroslužbu, která se dobře škáluje od několika připojených zařízení až po rozsáhlé systémy. Samozřejmostí je compliance, tedy soulad s aktuální kyberbezpečnostní legislativou.

SeaCat PKI je kompatibilní s hardwarovými bezpečnostními moduly (HSM) a podporuje klíče CA založené na HSM. Lze ji tedy použít pro řešení, která vyžadují maximální úroveň ochrany klíčů.

Své využití najde např. v oblasti zdravotnictví a zdravotnické techniky (telemedicína, zdravotnická zařízení IoT nebo moderní chytrá nemocniční zařízení) či průmyslu (správa klíčů a certifikátů pro jakékoli připojené průmyslové zařízení).

Díky možnosti využít SeaCat PKI i jako službu odpadá i složitá implementace. To znamená, že není třeba nic instalovat, konfigurovat a udržovat. Stačí si jen službu předplatit a během pár okamžiků lze používat nejsilnější možné kybernetické zabezpečení pro mobilní aplikace nebo zařízení IoT.

Více na sales@teskalabs.com; www.teskalabs.com; logman.io a na sociálních sítích LinkedIn,

Facebook nebo X.

<https://www.ceskenoviny.cz/tiskove/zpravy/jak-zajistit-bezpecnou-komunikaci-v-digitalnim-prostredi-odpovedi-je-pki/2469945>