Budoucnost osobních dokladů? Vyšší bezpečnost a odolná kryptografie

5.5.2025 - | PROTEXT

Biometrické prvky se staly nedílnou součástí cestovních dokladů. Pasy a Občanské průkazy obsahují otisky prstů i sken obličeje. „Dnešní doklady už nejsou jen kusem plastu, ale sofistikovaným nositelem biometrických dat, která pomáhají rychlé a bezpečné identifikaci," vysvětluje Lukáš Pugner.

„Na letištích dnes vidíme automatizované systémy, jako jsou E-Gates, které využívají rozpoznání obličeje pro urychlení pasové kontroly. Dalším trendem je DTC Digital Travel Credentials, Digitální cestovní identita (DTC) podle standardů ICAO (Mezinárodní organizace pro civilní letectví), která změní přístup k cestování."

Občanské průkazy se vyrábějí z polykarbonátu, který je odolnější a tím je zaručena jeho životnost po dobu platnosti. *„Moderní bezpečnostní prvky, jako jsou laserové gravírování, patří mezi velmi účinné ochranné prvky proti padělání a v kombinaci s elektronickou částí dokladu, která je personalizována při výrobě, zajišťuje vysokou úroveň bezpečnosti."*

Viditelné ochranné prvky se staly běžnou součástí osobních dokladů, ale jejich vizuální podoba se průběžně inovuje tak, aby byly i nadále obtížně padělatelné.

Evropská unie pracuje na standardizaci elektronické identity v rámci nařízení eIDAS 2.0. Cílem je sjednocení identifikačních systémů pro online služby a přeshraniční ověřování totožnosti. Například využití systémů jako EES (Entry/Exit System) nebo ETIAS pro sledování vstupu do Schengenu. Nově bude zaváděna i EUDIW (evropská peněženka digitální identity).

„Díky jednotné evropské identitě se občané budou moci snadno prokázat a v budoucnu i přihlásit do online služeb v jakékoli členské zemi. To zjednoduší řadu administrativních procesů a zvýší bezpečnost při ověřování totožnosti," vysvětluje Lukáš Pugner.

Jednou z největších výzev budoucnosti je přechod na postkvantovou kryptografii (PQC). Kvantové počítače mohou prolomit současné šifrovací algoritmy, a proto se vyvíjejí nové kryptografické technologie odolné vůči těmto hrozbám.

Lukáš Pugner upozorňuje: *„Je nezbytné začít implementovat kvantově bezpečné algoritmy již nyní, abychom ochránili osobní data v budoucnosti. PQC najde využití v technologiích elektronických podpisů, šifrování osobních údajů a bezpečné autentizaci."*

„Osobní doklady obsahují celou řadu citlivých údajů," doplňuje Lukáš Pugner. *„Právě proto bude v blízké době nezbytné implementovat nové postkvantové kryptografické algoritmy, které nahradí dosavadní standardy, jako jsou RSA nebo ECDH. Algoritmy jako ML-DSA nebo ML-KEM, které jsou standardizovány americkým úřadem NIST, zajistí, že doklady zůstanou chráněné i v době kvantových počítačů a zabrání jejich padělání nebo neautorizovanému čtení."*

Moderní digitální doklady se postupně stanou standardem a implementace nových kryptografických technologií zajistí jejich dlouhodobou bezpečnost. Proto má smysl již nyní plánovat migraci na kvantově bezpečné technologie. K tomuto kroku vyzývají i evropské bezpečnostní agentury, které ve společném prohlášení zařadily migraci na PQC mezi hlavní priority.

„Státy by měly již nyní plánovat přechod na kvantově bezpečné technologie, aby jejich identifikační systémy zůstaty chráněné i za několik desetiletí. My sami jsme se aktivně zapojili do výzkumu těchto technologií a jejich aplikace pro eGovernment. Jsou nezbytné pro dlouhodobou bezpečnost osobních dokladů," uzavírá Lukáš Pugner.

https://www.ceskenoviny.cz/tiskove/zpravy/budoucnost-osobnich-dokladu-vyssi-bezpecnost-a-odolna-kryptografie/2669168