



# NAKIT

Národní agentura pro  
komunikační a informační  
technologie, s. p.

V Praze 28. června 2021

## **Průvodce světem elektronické identity: Odborníci z MV ČR, NAKIT a AFCEA zveřejnili společně vytvořený dokument „Doporučení pro bezpečné nakládání s e-identitou“.**

S rozvojem služeb eGovernmentu a narůstající potřebou využívání elektronických služeb v běžném životě je stále častěji využívána *elektronická identita*. Odborníci na systémy eGovernmentu z Ministerstva vnitra, kybernetickou a informační bezpečnost z NAKIT a české pobočky neziskové a vzdělávací organizace AFCEA (Armed Forces Communications & Electronics Association) proto společně vydali dokument s názvem **Doporučení pro bezpečné nakládání s e-identitou**, který má veřejnost informovat, pomoci zorientovat se v právním vymezení a zákonném ukotvení tohoto pojmu a upozornit na bezpečnostní rizika.

V úvodu dokument definuje, co je a co není e-identitou ve smyslu zákona, tedy státem garantovaného digitálního ověření totožnosti. Dále pak seznamuje s úrovněmi záruk, které různé prostředky poskytující e-identifikaci dle způsobu ověření a zabezpečení nabízí.

Hlavními výhodami získání a využívání e-identity jsou v první řadě zrychlení komunikace občana se státem, díky dvoufaktorovému systému ověřování také zlepšení bezpečnosti a z ní vyplývající větší ochrana soukromí. E-identitu může občan získat pomocí elektronických identifikačních prostředků poskytovatelů, kteří získali akreditaci od Ministerstva vnitra a jsou napojeni na NIA (Národní bod pro identifikaci). Takovými prostředky jsou v současné chvíli Mobilní klíč eGovernmentu, eObčanka, NIA ID, I.CA, mojeID a nedávno zprovozněná služba bankovních institucí Bankovní identita, přičemž každý z prostředků nabízí různé druhy využití a vlastní specifika při ovládání v mobilním prostředí. Služeb a možností, jak e-identitu využít, v současné době skokově přibývá. Místem, kde lze přehled těchto služeb nalézt, je například **Portál občana**, elektronické centrální místo vstupu ke službám eGovernmentu vytvořené Ministerstvem vnitra a NAKIT.

S využíváním e-identity se ale pojí i rizika jejího zneužití neoprávněnými osobami, a proto je při zacházení s tímto druhem identity třeba dodržovat bezpečnostní zásady jako při jakékoliv jiné činnosti. Dokument tak uživatelům radí i to, jak rizikům předcházet a jak se v případě ztráty či zneužití e-identity bránit. V závěru dokumentu pak nalezneme přehled nejčastějších otázek týkajících se e-identity a odpovědi na ně.



# NAKIT

Národní agentura pro  
komunikační a informační  
technologie, s. p.

*„V poslední době roste využití i význam elektronické identity při komunikaci se státem. Napříč sektory jsme cítili společnou potřebu jasnou a srozumitelnou formou občanům představit zásady jejího používání, objasnit výhody, které přináší, ale také upozornit na možná rizika a poradit, jak se s nimi vypořádat.“ říká Vladimír Rohel, ředitel sekce Bezpečnost NAKIT a dodává: „V dokumentu se snažíme poskytnout veřejnosti první pomoc při orientaci v mnohdy na první pohled nepřehledném prostředí definic, termínů a bezpečnostních podmínek. Jde o to lidem nabídnout dostatek přehledných informací, aby dokázali e-identitu využít ve svůj prospěch a usnadnit si tím život, a to hlavně na poli komunikace s úřady. Spolupráce s kolegy z ostatních organizací na tomto dokumentu zafungovala výborně. Měli jsme všichni stejný cíl i představu, jak ho dosáhnout. Všem kolegům z partnerských organizací za jejich skvělou spolupráci moc děkujeme.“*

Dalšími partnery, kteří se na tvorbě dokumentu podíleli, jsou Národní úřad pro kybernetickou a informační bezpečnost, Vojenské zpravodajství, Bezpečnostní informační služba, Úřad pro zahraniční styky a informace, CZ.NIC, Bankovní identita a.s., Česká bankovní asociace, Správa základních registrů a První certifikační autorita, a.s.

Lukáš Trnka, tel.: 602 282 653, e-mail: [lukas.trnka@nakit.cz](mailto:lukas.trnka@nakit.cz)