

# PKCS standardy pro potřeby zdravotnické dokumentace

Josef Špidlen, Miroslav Nagy

*EuroMISE centrum,  
Ústav Informatiky AV ČR, Praha, Česká republika*

## Abstrakt:

*V rámci výzkumu oddělení medicínské informatiky ÚI AV ČR se zabýváme reprezentací medicínských informací a vývojem tzv. elektronického zdravotního záznamu. Ve snaze uvést myšlenky a vyvinuté přístupy do praxe ve zdravotnictví byla navázána spolupráce s několika výrobci nemocničních informačních systémů. Společně s nimi pracujeme na projektu „Informační technologie pro rozvoj kontinuální sdílené péče o zdraví“, ve kterém je třeba řešit zabezpečení citlivých medicínských dat a další bezpečnostní otázky v souladu s platnou legislativou. Dílčími úlohami jsou spolehlivá autentifikace každého účastníka řetězce poskytování zdravotní péče, bezpečné podepsání elektronické zdravotní dokumentace zaručeným elektronickým podpisem a zpětné jednoznačné ověření původního autora dokumentace. Pro řešení těchto úloh je vhodné využít externí kryptografické zařízení. Výhoda kryptografického zařízení je např. v tom, že soukromá část asymetrického klíče je vygenerována přímo zařízením a nikdy jej neopustí, což napomáhá bezpečné identifikaci autora elektronického podpisu. Abychom předešli úzké vazbě na konkrétní kryptografické zařízení, je vhodné využít existujících standardů pro komunikaci s těmito zařízeními. Představiteli těchto standardů jsou například rodina standardů PKCS či MS CAPI. Text článku se převážně zabývá právě úvodem do kryptografického standardu PKCS #11 a možnostmi jeho využití pro účely projektu.*

**Klíčová slova:** kryptografické standardy, zdravotnická dokumentace, PKCS

## Adresa pro korespondenci

Josef Špidlen, EuroMISE centrum,  
Ústav Informatiky AV ČR,  
Pod Vodárenskou věží 2, 182 07 Praha 8, Česká republika  
Email: spidlen@euromise.cz