

## Kontaktní karty

Karty mohou mít různé kontaktní čipy. Úplně jednoduché, které jsou v podstatě paměťovým médiem s pamětí desítky a stovky bytů bez operačního systému až po současné „inteligentní“ (smart) čipy s vlastním operačním systémem, pamětí desítek kilo bytů a vlastními kryptografickými koprocesory. Mezi takové čipy patří i SIM karta, která ovšem nedosahuje takových parametrů jako nejlepší čipové karty (např. od společnosti SafeNet Inc.).

Přístup k těmto kartám je chráněn heslem (PIN), který zná vlastník karty. Jedná se tedy o dvoufaktorovou bezpečnost: něco, co máte (Vaše čipová karta) a něco, co znáte (Vaše heslo – PIN). Nikdo se nemůže dostat k Vaším důvěrným informacím, aniž by měl Vaši kartu a současně znal heslo. Nejlepší čipové karty podporují PKI, elektronickou autorizaci dat (elektronický podpis) a šifrování (symetrické i asymetrické). Tyto čipové karty jsou schopny ve svém koprocesoru generovat šifrovací klíčové páry a provádět s nimi veškeré požadované operace, a tak privátní klíč nikdy neopustí tuto kartu a není možné jej odchytnout (odposlechnout) cestou po síti či v PC.

Dostatečně velká paměť EEPROM umožňuje ukládání digitálních certifikátů, využívaných pro autentizaci uživatele do PC, sítě, VPN a k aplikacím, šifrování komunikace a elektronický podpis pošty, dokumentů i webových formulářů. Čím je paměť větší, tím více certifikátů i dalších informací (hesla, atd.) se na kartu vejde. Toto je důležité hlavně při nasazení v infrastruktuře veřejných klíčů, kdy se na kartě mohou nechat uložené i certifikáty po době platnosti, a tak zajistit, že si bez problémů přečtete i staré zašifrované dokumenty. Vaše digitální certifikáty jsou v mnohem větším bezpečí na čipové kartě než na harddisku Vašeho počítače nebo na disketě. Lze jich samozřejmě využít i jako elektronickou peněženku nebo pro věrnostní programy. Nejnovější čipové karty (JavaCard) lze použít jako platební kartu dle standardu EMV (rezidentně uložený aplet VISA) nebo na kartu uložit vlastní Java aplety.

**Pro komunikaci s čipovou kartou je potřeba kontaktní čtečka čipových karet a speciální software.**