



Profesionální elektronická identita

na čipové kartě



- efektivní řešení vnitrofiremní IT bezpečnosti
 - nativní integrace do prostředí Microsoft
- základní koncept postavený na technologii PKI
 - možnost použití i mimo PKI architekturu (jednoduchá Single Sign-on aplikace)



Cryptoplus ProID je Vaše elektronická identita na čipové kartě. Podpora a nativní integrace CryptoPlus ProID do produktů společnosti Microsoft nabízí snadné vybudování PKI systémů ve Vaší organizaci.

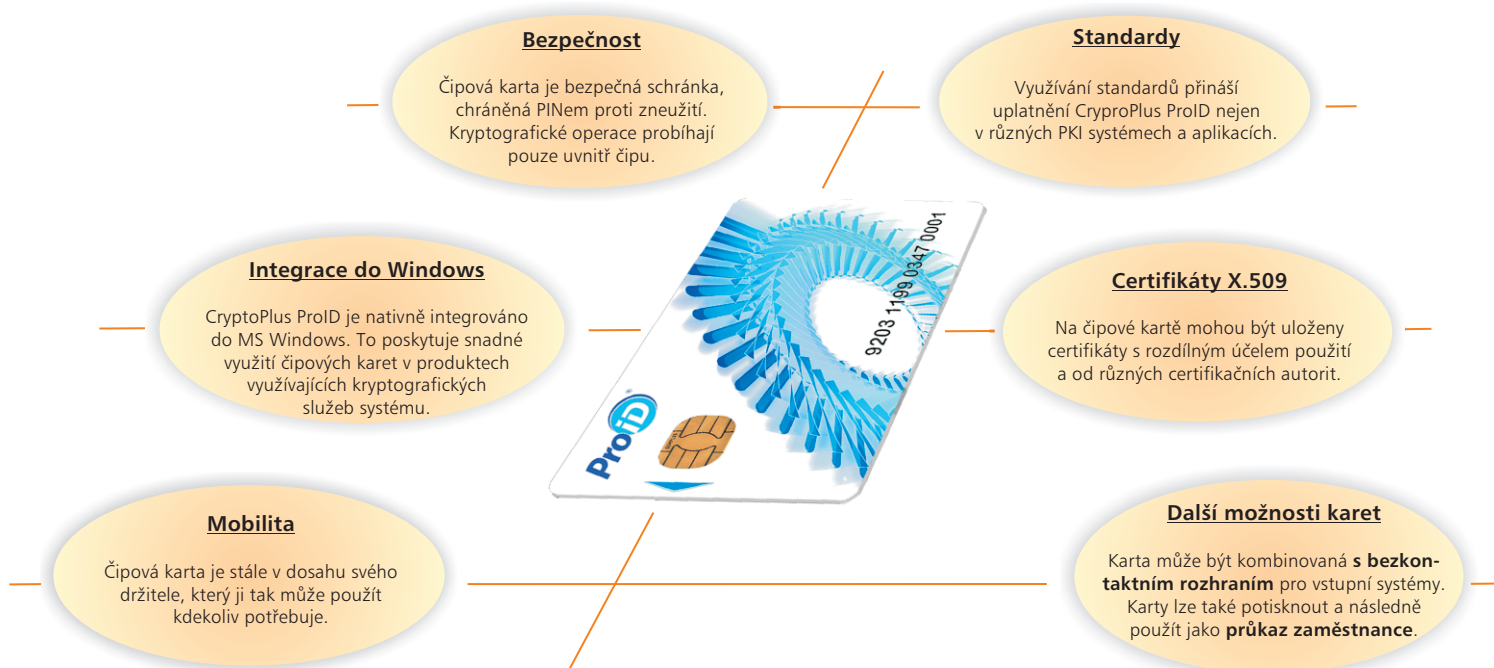
S pomocí CryptoPlus ProID můžete jednoduše budovat bezpečné informační systémy. Architektura CryptoPlus ProID založená na využívání standardů nabízí široké aplikační využití v rámci informačních technologií ve Vaší organizaci. Ochrana dat na kartě pomocí PIN přináší jednoduché řešení zabezpečení IT.

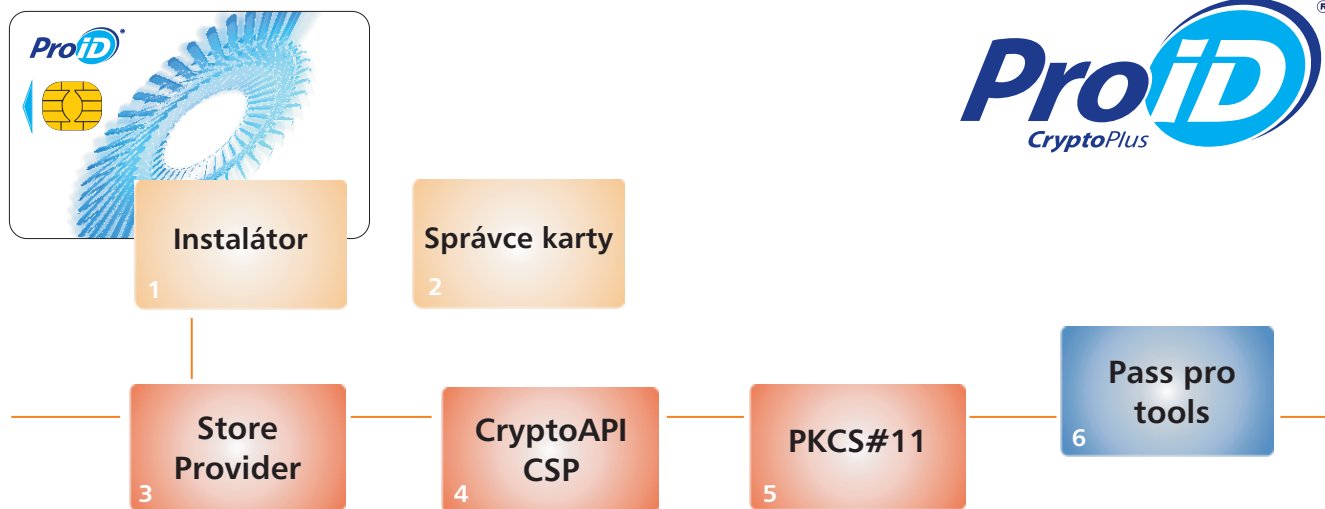
CryptoPlus ProID můžete použít pro:

- **autentizaci**
 - do počítačů a sítí
 - na internetové servery
 - vzdálený přístup do sítě
 - do dalších aplikací
- **zabezpečení dokumentů**
 - elektronické podepisování dat a e-mailů
 - (de-)šifrování dat a e-mailů
- **bezpečné uložení citlivých aplikačních dat**
- **mnoho dalších funkcionalit**

Na čipové kartě ProID mohou být uloženy elektronické identity - tedy příslušné RSA klíče a jejich certifikáty ve standardu X.509 vydané různými certifikačními autoritami.

CryptoPlus ProID také využijete i v systémech, které nepodporují PKI. To vše s pomocí vlastní Single Sign-on aplikace PassPro Tools. Typicky pro přihlášení do skladových, objednávkových nebo ekonomických SW.





Čipová karta ProID - bezpečný nosič elektronických identit. Kryptografické operace probíhají pouze v čipu karty. Karta může být potištěna či kombinována s dalšími technologickými prvky, např. s bezkontaktním čipem pro docházkové a vstupní systémy nebo k potištění jako průkaz zaměstnance.

1 Instalátor - zajistí korektní nastavení PC, aby mohlo být řešení CryptoPlus ProID bezproblémově používáno. Kromě obvyklých instalačních procesů zahrnuje kontrolu a nastavení systémových komponent PC/SC.

2 Správce karty - přehledně zobrazuje obsah karty s maximálním komfortem obsluhy. Zajišťuje funkce lokální správy karty (export veřejných údajů, import klíčů a certifikátů, odblokování či změnu PIN, změnu PUK, atp.). V případě potíží dokáže poradit optimální postup řešení, pro komplikovanější případy je možné vygenerovat log pro pracovníky zákaznické podpory.

3 Store Provider - zajistí automatické zaregistrování certifikátů z karty do systému MS Windows. Uživatel není nucen ručně registrovat uložené certifikáty. Stačí vložit kartu do čtečky a za několik okamžiků je možné certifikáty na kartě používat.

4 CryptoAPI CSP (Cryptographic Service Provider) - základní kryptografická komponenta CryptoPlus ProID. CSP nativním způsobem rozšiřuje kryptografické funkce MS Windows (CryptoAPI). Uživatelé mohou používat PKI v existujících aplikacích, ale využívat i nových funkcionalit, které přímo vyžadují použití čipových karet (např. Windows Smart Card Logon - přihlášení k PC pomocí karty).

5 PKCS#11 - tato specializovaná kryptografická knihovna je používána zejména v multiplatformním prostředí. Typicky Win + Linux. Vysoká míra interoperability zajišťuje použití v mnoha aplikacích, jejichž společným atributem je bezpečnost.

6 PassPro Tools - jednoduchá Single Sign-on aplikace, pro potřeby přihlášení s použitím statických autentizačních údajů, např. jména a hesla. Tato aplikace nejen chrání přihlašovací údaje uložené bezpečně na kartě, ale zároveň s nimi umožní i automatické přihlášení.

■ Přehled vybraných funkcionalit CryptoPlus ProID

Aplikace	Verze	Použití	Poznámka
Internet Explorer	5.5 a vyšší (včetně 7.0)	Žádost o certifikát a instalace certifikátu	Podporuje interface vyžadovaný objektem enroll pro vytváření žádosti o certifikát a pro následné uložení certifikátu na kartu.
		Klientská autentizace na www pomocí SSL	V systému musí být platný certifikát uznávaný Web serverem.
Outlook Express Windows Mail - Vista	5.5 a vyšší	Elektronický podpis	V systému musí být platný certifikát pro daný typ zabezpečení.
		Šifrované zprávy	V systému musí být platný certifikát pro daný typ zabezpečení.
MS Outlook	2000, 2003 a vyšší včetně 2007	Elektronický podpis	<ul style="list-style-type: none"> ■ Musí být nastaveno zabezpečení typu S/MIME (nepracuje se zabezpečením Exchange Server Security). ■ V systému musí být platný certifikát pro daný typ. zabezpečení.
		Šifrované zprávy	
MS Office	2000, XP	Elektronický podpis maker	V systému musí být platný certifikát pro daný typ operace.
	XP, 2003, 2007	Elektronický podpis dokumentů	V systému musí být platný certifikát pro daný typ operace.
		Šifrování dokumentů	Pouze na bázi symetrické kryptografie.
Windows	2000, XP, 2003, Vista - 2008	Přihlášení do systému - Smart Card Logon	<ul style="list-style-type: none"> ■ Vyžaduje doménový server s CA (popř. alternativní konfiguraci serveru). ■ Na kartě musí být platný certifikát uznávaný CA domény. ■ Klienti Windows 2000, XP Professional, Vista Business a vyšší.
	Terminal Server 2000, 2003, 2008	Přihlášení do systému	<ul style="list-style-type: none"> ■ Klienti Windows 2000, XP Professional, Vista Business a vyšší. ■ Vyžaduje speciální SW modul na straně klienta (je k dispozici).
	VPN, RAS	EAP autentizace čipovou kartou	Na kartě musí být platný certifikát pro daný typ zabezpečení.
Internet Explorer Mozilla Firefox Thunderbird	5.5 a vyšší (včetně 7.0)	Žádost o certifikát a instalace certifikátu Klientská autentizace na www pomocí SSL Elektronický podpis formulářů a e-mailů Šifrování dat	V systému musí být platný certifikát pro daný typ operace. Podpora přes rozhraní PKCS#11, PKCS#7, SPKAC, S/MIME.



e-mail: obchod@monetplus.cz, proid@monetplus.cz



www.monetplus.cz
www.proid.cz

MONET+, a. s.

Za Dvorem 505, 763 14 Zlín-Štípa, Česká republika



tel: +420 577 110 411, fax: +420 577 914 557