Čipové karty a USB tokeny, aneb bezpečnější autentizace a šifrování (1) - účel čipových karet a USB tokenů

"Čipová karta" a "USB token" obsahují stejný čip, tak jaký je v nich rozdíl? To se dozvíme v našem novém seriálu. Je určen pro všechny, kteří se přihlašují do operačního systému, k VPN, bezpečnému webu, používají eBanking, šifrují, či digitálně podepisují emaily nebo soubory..., prostě pro všechny, kterým není bezpečnost jejich důležitých dat lhostejná.

"Čipová karta" a "USB token" obsahují stejný čip, tak jaký je v nich rozdíl? To se dozvíme v našem novém rozsáhlém seriálu. Je určen pro všechny, kteří se přihlašují do operačního systému, k VPN, bezpečnému webu, používají eBanking, šifrují, či digitálně podepisují emaily nebo soubory..., prostě pro všechny, kterým není bezpečnost jejich důležitých dat lhostejná.

Nejprve si pojďme stručně povědět o tom, jakým způsobem nám tyto bezpečnostní předměty - "tokeny" pomůžou o řád zvýšit bezpečnost autentizace a šifrování.

Pokud jsou pro Vás pojmy jako "certifikát", "privátní klíč" nebo "asymetrická kryptografie" španělskou vesnicí, doporučuji k přečtení na příklad kraťoučký, český úvod do této problematiky na stránkách 1.Certifikační Autority - ICA.

Pozn. redakce - další informace na našem webu:

Pravdy o elektronickém podpisu a šifrování

SSL protokol

Základní slovníček z kryptografie

Kam ukládat šifrovací a privátní klíče?

Představme si situaci, kdy chcete zašifrovat data na Vašem počítači. Použijete k tomu ten nejlepší šifrovací software s tou nejbezpečnější šifrou! Vaše data jsou bezpečně zašifrována a měl by se k nim dostat jen ten, kdo zná šifrovací klíč. Kde je tento klíč uložen? No, samozřejmě také někde na hard disku. A jak je tam uložen? Aby to bylo nějak bezpečně, uživatel se k šifrovacímu softwaru přihlašuje většinou jménem a heslem. Tedy šifrovací klíč je ještě "přešifrován" nějakým způsobem v závislosti na Vámi zadaném hesle. No, a dostáváme se ke kameni úrazu!

Celá bezpečnost Vašich dat je závislá nikoli na téměř neprůstřelném software a nejlepší šifře, ale na Vámi zvoleném hesle! To je velmi dobrý důvod, proč ukládat šifrovací klíče mimo HDD na nějaké "bezpečné!" zařízení. Někam, kam se na něj případný útočník bude dostávat jen velmi těžce. Na nějaké zařízení, které budete pokud možno nosit neustále s sebou, takže budete mít nad přístupem k těm pár vysoce důležitým bitům plnou kontrolu. Na příklad na čipovou kartu, nebo USB token.

Nejde jen o šifrovací klíče, to samé v bledě modrém jsou privátní klíče pro digitální podpis, přístup k VPN, k logování do operačních systémů... Jeden ze známých českých útoků na systém openPGP (systém určený pro digitální podepisování/šifrování emailů) nespočíval v ničem jiném, než v útoku na privátní klíč uložený na hard disku počítače.

Někteří uživatelé tvrdí, že si svůj šifrovací klíč, nebo svůj privátní klíč ukládají na disketu, nebo USB flash disk, a že je to prý to samé, jako čipové karty ;-) Není, rozhodně není! A tento článek Vás o tom přesvědčí. Navíc Vám umožní vybrat to nejvhodnější řešení pro uložení Vašich "tajných bitů" (šifrovací klíče mají většinou jen několik stovek bitů a privátní klíče několik Kbitů).

Autentizace pomocí jména a hesla - přežitek

Autentizace je ověření identity uživatele. Autentizace pomocí hesla, by měl být v dnešní době již spíše přežitek. Uživatelé zadávající své username a heslo, jsou noční můrou každého správce sítě, který dbá na bezpečnost.

1. Uživatelé volí hesla typu: rodné číslo, jméno partnera/-ky, telefonní číslo, nápisy poblíž počítače..., **tedy hesla, která může útočník snadno uhádnout** .
2. Obyčejná slova, typu domeček, sluníčko, krteček nejsou o nic lepší. **Slovníkový útok**se slovníkem o 30 tis. slovech je pořád rychlejší než vyzkoušet všech 78 miliard kombinací u 7 znakového hesla (znaky a-z, 0-9).
3. Heslo se dá snadno získat **odpozorováním** , obzvláště u lidí, kteří nepíší všemi deseti a s využitím moderní techniky. S web kamerami, mobily třetí generace, či digitálními fotoaparáty s možností krátké video sekvence to není až tak veliký problém.
4. Pokud odhlédneme od hesel do operačního systému, dají se všechna ostatní hesla (k emailu, informačnímu systému, účetnímu software...) **odchytit na úrovni klávesnice.** Napsat v paměti rezidentní program, který bude ukládat do souboru všechny stisknuté znaky na klávesnici, **je úkol pro začínajícího programátora, tedy většinu středoškoláků!!** Neumíte-li programovat, kupte si nějaký software, který to umí - na příklad iBoss. Tento software zaznamenává vše, co uživatel na počítači dělá, včetně všech stisknutých kláves s podrobným výpisem v jaké to bylo aplikaci, webové stránce... Nebo si stáhněte nějaký jednodušší freeware na internetu. Pokud máte jen trochu mocnější práva ve vaší podnikové síti, dokážete získat snad všechna hesla všech uživatelů ke všem firemním systémům, a to nemusíte umět ani programovat!

Myslím, že nemá cenu, abych Vás dále přesvědčoval o tom, že je v dnešní době lepší použít pro autentizaci něco bezpečnějšího! Důvodů, proč nepoužívat statická hesla by se asi našlo více.

Ve Windows 2000 lze stanovit, že heslo musí být dlouhé minimálně 8 znaků, musí obsahovat znaky minimálně z tří skupin ze čtyř (velké znaky, malé znaky, číslice a speciální znaky) a že třeba po 5 špatných pokusech se účet uživatele zablokuje na x minut.

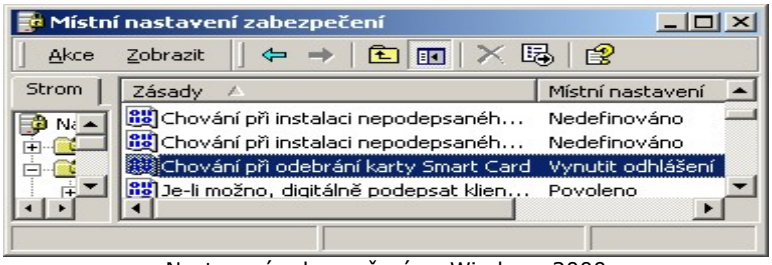
Windows Smart Card Logon

To všechno lze, ale bodu 3. a 4. se u většiny softwaru stejně nevyhnete. Odpozorování hesla se nevyhnete ani u operačního systému! Proto už i ve Windows 2000 je něco, co se nazývá Smart Card Logon. Uživatel tak pro přihlášení potřebuje hned dvě věci (dvoufaktorová autentizace):

1. Čipovou kartu, či USB token se svým privátním klíčem a certifikátem.
2. Heslo/pin k tokenu, který je takto chráněn proti zneužití při krádeži, či ztrátě.

Přihlašovací obrazovka, vyzývající uživatele k zasunutí tokenu

Když už jsem u autentizace do Windows pomocí tokenů... Lze odstranit, nebo alespoň podstatně eliminovat další nešvar uživatelů. Ti se často vzdálí od svého počítače na delší dobu, aniž by se odhlásili, či alespoň uzamknuli stanici. Lze nastavit, co se stane po vysunutí čipové karty, či USB tokenu ze slotu. Uživatel odcházející z kanceláře si vezme svoji čipovou kartu potřebnou i pro otevření dveří, či USB token, který má na svazku svých klíčů, a tím se stanice buď automaticky uzamkne, či dojde přímo k odhlášení uživatele. Hezké ne? ;-) Více o přihlašování do Windows, či jiných operačních systémů si povíme někdy jindy. Pokud Vás přihlašování do Windows zaujalo a nechcete čekat na "někdy jindy", za celkem zajímavý považuji dokument (1,4MB) od Amerického Bezpečnostního Úřadu - NSA, který není tajný ;-)



Nastavení zabezpečení ve Windows 2000

Další způsoby autentizace

Dvě věci jsou více než jedna a tak je tato možnost autentizace považována za řádově bezpečnější, než pouhé používání hesel.

Snímač otisku prstů integrovaný do myši

Autentizační kalkulátor

USB token se snímačem otisku prstu

Čtečka čipových karet ve formě PC Card

Některé z dalších předmětů pro autentizaci

Jsou samozřejmě i jiné řešení autentizace, jako jsou **autentizační kalkulátory, zaslání jednorázového kódu ve formě sms** na mobil klienta, **snímače otisků prstů, analyzátory DNA** a mnoho dalších. Těmito řešeními bych se chtěl zabývat až na úplném závěru a ne příliš do hloubky. Chtěl bych zde hlavně srovnat čipové karty a USB tokeny. Proč? Protože jsou to jedny z mála řešení, která umožňují nejen bezpečnou autentizaci, ale také slouží jako velmi bezpečná úložiště malých (řádově několik kB) dat, která se snažíme před útočníky chránit. Dat, jako jsou hesla, šifrovací klíče, privátní klíče, sdílená tajemství, certifikáty, kódy atd. Čipové karty a USB tokeny jsou tedy velmi univerzální, i když se najdou situace, kde jsou ku příkladu autentizační kalkulátory, či jiná řešení mnohem výhodnější. Ale i k tomu se dostaneme.

Tyto tokeny Vám tak pomohou k bezpečnějším VPN, přihlašování do operačního systému, digitálnímu podpisu a šifrování emailů/souborů, bezpečnějšímu eBankingu, přístupu k webu...

V dalších dílech se podíváme na to, v čem se USB tokeny a čipové karty liší, a naopak, co mají společného.

Čipové karty a USB tokeny, aneb bezpečnější autentizace a šifrování (2) - metody autentizace

Pojďme se nejprve podívat na rozdělení metod autentizace. Tedy toho, jakým způsobem můžeme ověřovat uživatelovu identitu. Není totiž token, jako token... Pod pojmem dvoufaktorová autentizace rozumíme současné užití dvou různých metod – faktorů. Jedna z možností – „token + heslo", nás bude zajímat v tomto článku.

Pojďme se nejprve podívat na rozdělení metod **autentizace**. Tedy toho, jakým způsobem můžeme ověřovat uživatelovu identitu. Není totiž token, jako token...

1. **Znalost** - Uživatel se prokáže **znalostí**, kterou **„by měl"** vědět pouze on, typicky heslo, šifrovací klíč uložený na disku, vstupní PIN...
2. **Vlastnictví** - Autentizovat se může pouze ten, kdo vlastní nějaký předmět - **token**. Na příklad: autentizační kalkulátor, čipová karta, USB token...
3. **Biometrika** - Měří se tzv. **biometrické vlastnosti** uživatele – otisky prstů, geometrie ruky, oční sítnice, tvar obličeje, rozpoznávání řeči, test DNA...

Pod pojmem **dvoufaktorová autentizace** rozumíme současné užití dvou těchto různých metod – faktorů. Jedna z možností – „token + heslo", nás bude zajímat v tomto článku. **Třífaktorová autentizace** je potom využitím tokenu, znalosti i biometriky dohromady.

To, že je "dvoufaktorová autentizace" něco víc, naznačuje už samotný název. Na druhou stranu, nelze jakkoli srovnávat "jednofaktorovou" autentizaci pomocí duhovky oka za 2 tisíce dolarů a "dvoufaktorovou" autentizaci pomocí tokenu a hesla za 50 dolarů ;-)

Základní možnosti autentizace:

	A	B	C	D	E	F	G
Znalost	x			x		x	x
Token		x		x	x		x
Biometrika			x		x	x	x

Možnost A - o tom, že to v dnešní době není dobrý nápad, jsme se bavili již v prvním díle ;-).

Možnost B - patří sem hlavně různé bezkontaktní tokeny a karty s magnetickým proužkem, které nejsou zabezpečeny žádným pinem/heslem. Při krádeži může být předmět kýmkoli zneužit! Většinou je navíc možné předmět i poměrně jednoduše duplikovat. Tyto tokeny se využívají spíše pro zabezpečení objektů, v docházkových systémech a pod. Dnes se pro tyto účely poměrně hojně využívá bezkontaktních čipových karet.

Možnost C - je první rozumnou variantou k využití pro autentizaci ve světě počítačů. Levnější snímače otisků prstů, ale nijak zvlášť bezpečné nejsou (jako příklad - jeden z mnoha dokumentů, jak obejít levný snímač otisků prstů). Existuje však celá řada dalších biometrických metod. Některé z nich se používají i v prostředích „přísně tajné" (příkladem nechť je snímač duhovky oka). Těmto řešením se ale v článku věnovat nebudeme.

Snímač duhovky oka

Snímač geometrie ruky

Zbývají nám pouze možnostmi **D, E nebo G**, protože pouze tyto možnosti obsahují token, který je zabezpečen proti zneužití při ztrátě, či krádeži.

Možnost D je typicky realizována čipovou kartou, USB tokenem nebo autentizačním kalkulátorem. Uživatel se prokazuje vlastnictvím tokenu a přístup k tokenu je navíc chráněn heslem/pinem. Kalkulátor nám bohužel neposlouží jako bezpečné úložiště šifrovacích klíčů, či jiných "tajemství". Jinak má kalkulátor mnoho výhod, viz. dále. Základní idea autentizačního kalkulátoru je ta, že uživatel zadá heslo/PIN a po zadání kalkulátor vygeneruje jednorázové přístupové (po každé jiné) heslo. **Právě čipovými kartami a USB tokeny z této oblasti se budeme zabývat.**

Možnosti E a G, kdy se autentizujeme vůči tokenu biometrickou veličinou, nejčastěji otiskem prstu, nebo otiskem prstu a heslem, zde uvažovat nebudeme. Zvláště použití všech tří faktorů je více finančně náročnější než dvoufaktorová autentizace pomocí tokenu a hesla. Většina čipových karet a USB tokenů, které se dnes nasazují, jsou chráněna heslem, či pinem.

USB token s autentizací pomocí otisku prstu

Čtečka čipových karet se snímačem otisku prstů

Důvody, proč se tato řešení příliš nenasazují jsou asi tyto. Vyšší **cena**, obecné povědomí o**ne příliš velké bezpečnosti** levných snímačů otisků prstů a hlavně samotná **podstata biometriky**.

Pokud se použije kvalitní snímač, tak máte na krku manažera, který bude tlačit zase na menší cenu :-(Pokud spravujete 400 uživatelských účtů, víte o čem hovořím.

Podstatou biometriky mám namysli asi toto: Snímač získá otisk prstu a ten se potom porovnává.

- První problém je to, kde k porovnání dojde. Čipová karta, či USB token nemusí být pro porovnání otisků uzpůsobené. Váš vzorek otisku je pak v lepším případě uložen na kartě, ale porovnání provádí software na Vašem počítači, na který lze zaútočit. V tom horším případě je vzorek uložen na Vašem počítači, nebo dokonce v databázi na nějakém serveru.
- Druhý problém je ten, že porovnání dvou hesel o 8 znacích je exaktní a bez problému. Porovnání dvou otisků prstů zas tak triviální není. Čím více nastavíte systém tak, aby jste snížili pravděpodobnost přijetí podvrženého otisku, tím více zvýšíte pravděpodobnost, že systém odmítne i oprávněného uživatele. A naopak. Čím více nastavíte systém tak, aby k odmítání oprávněných uživatelů nedocházelo, tím více šancí dáte útočníkovi.

Příště si již povíme o základních vlastnostech USB tokenů a čipových karet.

Čipové karty a USB tokeny, aneb bezpečnější autentizace a šifrování (3) - obecné požadavky na tokeny

V dnešním pokračování se podíváme na obecné požadavky kladené na tokeny, jako jsou např. odolnost předmětů vůči vnějším vlivům, odolnost konektorů a čtecího zařízení, mobilita, paměťová kapacita a na to, že tokeny se dají využívat i pro jiné účely, než které jsme si doposud naznačili - tj. ukládání "tajných" dat a autentizace.

V dnešním pokračování se podíváme na obecné požadavky kladené na tokeny, jako jsou např. odolnost předmětů vůči vnějším vlivům, odolnost konektorů a čtecího zařízení, mobilita, paměťová kapacita a na to, že tokeny se dají využívat i pro jiné účely, než které jsme si doposud naznačili - tj. ukládání "tajných" dat a autentizace.

1. Odolnost předmětů vůči vnějším vlivům

Předmět budeme neustále nosit při sobě. Je tedy důležité, aby byl token do určité míry odolný proti nárazům, lidskému potu, statické elektřině, elektromagnetickým polím, omáčkám, kávě, ... ;-) Důležité jsou i **provozní a skladovací teploty, max. vlhkost vzduchu**..., popřípadě zda se k předmětu prodávají nějaké obaly, pouzdra… Příkladem normy, která se tímto zabývá je **ISO 7816-1**. Norma definuje na příklad fyzické rozměry čipových karet, jejich odolnost proti statické elektřině a fyzickou odolnost při ohýbání karty. V této oblasti mají USB tokeny výhodu, neboť čip je chráněn plastovou skořápkou. Pouzdro u USB tokenu může být i vodotěsné. Zatímco USB tokeny standard ISO 7816-1 nepotřebují, u čipových karet je to nutnost, stejně jako splnění dalších částí této normy. Výrobci většinou uvádějí **ISO 7816-1 až 4** (méně známé části jsou 5 až 10). Pozn.: Abych Vás nemátl, normy 7816-2 a vyšší se již nezabývají odolností, ale jinými vlastnostmi čipových karet.

2. Odolnost konektorů a čtecího zařízení

Je dobré zjistit, jaká životnost je výrobcem garantována. Čipové karty, stejně tak čtečky vydrží jen určitý počet zasunutí (čipová karta například: až 10.000 zasunutí/vysunutí čipové karty). Tato hodnota je většinou dostatečně vysoká a proto je dobré se soustředit hlavně na hodnotu vlastní čtečky, než na hodnotu čipové karty. Obzvláště využívá-li počítač (tedy 1 čtečku) více uživatelů.

Čtecím zařízením u USB tokenů je vlastní port USB ve Vašem notebooku, či počítači. Při opotřebení by výměna nebyla dvakrát jednoduchá. Řešením je USB prodlužovací kabel, který stojí jen pár korun. Zároveň tím lze docílit stejného pohodlí, jako u čtečky čipových karet položené na stole (většina dnešních PC zatím nemá konektor USB vyveden na přední straně a bylo by nutné se ohýbat pod stůl ...). Navíc mají některé USB prodlužovací kabely (jako například UCB kabel) suchý zip pro upevnění na stůl a hezký design hodící se i na mahagonový stůl pana ředitele ;-) Životnost vlastního konektoru na USB tokenu je dána normou USB, ale u některých tokenů výrobci garantují až 50 000 cyklů vysunutí a zasunutí. S tím, že první chyby se začínají objevovat někde okolo 100 000 cyklů (na příklad tokeny iKey).

3. Mobilita

Pokud chceme využít řešení minimálně na několika místech, je nutné brát ohled na to, jaký hardware a software je k tokenu zapotřebí a jak jsou tyto složky „mobilní". Ovladačům a utilitám se asi nevyhneme. **U čipových karet je ale potřeba s sebou neustále nosit čtečku!** Zatímco USB tokeny čtečku nepotřebují, stačí USB port, který dnes najdete skoro na každém počítači. S **rostoucí oblibou portu USB** bude náskok USB tokenů v této oblasti vůči čipovým kartám stále větší. Již dnes se ve velkém vyrábějí základní desky s portem USB 2.0, který nabízí dostatečnou přenosovou rychlost pro většinu počítačových periférií (teoreticky až 60 MB/s). Očekává se tak ještě větší nárůst počtu PC, ve kterých nesmí chybět port USB.

Do starších PC je možné za několik set korun nainstalovat **PCI kartu – řadič USB**.

Už nějakou dobu se prodávají i tzv. **legacy free počítače**, které neobsahují žádné sériové, či paralelní porty, ale pouze "moderní" rozhraní jako jsou USB, FireWire (IEEE -1394), IR, bluetooth, ...

To, že se čtečky čipových karet vyrábějí v provedení jako PC Card, se sériovým rozhraním, USB rozhraním, či zabudované do klávesnice již ztrácí význam a USB tokeny jsou i v "mobilitě" podle mého názoru lepší, než čipové karty.

4. Víceúčelovost předmětů

Tokeny se dají využívat i pro jiné účely, než které jsme si doposud naznačili - tj. ukládání "tajných" dat a autentizace.

Čipové karty:

- ***Personalizace*** *- Na čipové karty lze natisknout jméno, fotografii držitele, čárkový kód a další údaje. Například řidičský průkaz jako čipová karta s fotkou a osobními nacionály + privátní klíč uložený na čipu jednoznačně určující řidiče. V praxi již toto řešení v několika státech na světě funguje.*
- ***Magnetický proužek*** *- Existují tzv. kombinované karty, které mají nejen smart čip, ale i magnetický proužek, který se využívá většinou pro stravovací služby, docházkový systém, přístup do objektu, ...*
- ***Bezkontaktní čip*** *- zde platí to samé, co pro magnetické proužky, s tou výhodou, že nedochází k opotřebení a je to i pohodlnější pro uživatele.*

USB tokeny:

Vzhledem k velikosti se na ně většinou tiskne unikátní sériové číslo, aby se na příklad poznalo, čí token se to vlastně ztratil. Jak si povíme dál, existují tokeny, do kterých se nedostane žádný administrátor, ale pouze a jen vlastní uživatel a je potřeba nějakým způsobem určit, komu nalezený token patří.

U velkých společností se spojují bezpečnost IT a bezpečnost objektu - budovy. V této oblasti mají čipové karty "plus", protože jsem zatím ještě nenašel řešení - USB token s bezkontaktním čipem pro docházkový systém. Natisknout fotografii na malý USB token je také "obtížné", o magnetické proužku nemluvě.

5. Paměťová kapacita

Abych nemusel stále opakovat "**privátní a veřejný klíč + certifikát/y**" budu na dále používat termín "**digitální ID** ", kterým budu myslet právě tyto 3 "části" asymetrické kryptografie.

Pokud budeme využívat předmět pro bezpečné ukládání digitálních ID a šifrovacích klíčů, hraje úlohu také kapacita paměti. Velikost digitálního ID pro digitální podpis se pohybuje typicky kolem 3kB (záleží na šifře, počtu a obsahu jednotlivých položek certifikátu). Vždy je potřeba počítat ještě s režií pro souborový systém na čipu. Komplexní profily pro bezpečnostní systémy jako je Entrust pak mohou na čipu zabírat i 6kB. Na druhou stranu můžete s Entrustem všechno - šifrovat data, zabezpečit emailovou komunikaci, přístup na web i k aplikačním serverům. Další místo na tokenu pak už není ani potřeba. Šifrovací klíče zabírají jen pár stovek bitů, takže u nich se o nedostatek místa už vůbec bát nemusíme (na příklad 128 nebo 256 bitů).

Standardně se dodávají čipové karty/ USB tokeny o velikostech 8, 16 a 32 kB. Pokud budeme token využívat na příklad pro přihlašování k Windows 2000 serveru, či VPN a ještě jako úložiště pro digitální identitu vystavenou na www.ica.cz, mělo by být 8KB postačující. Pozn.: 1.CA je zatím jediná certifikační autorita, díky jejímž kvalifikovaným certifikátům můžete komunikovat emailem i se státní správou.

Paměťový čip uvnitř není nezničitelný. Většinou je ale garantován minimální počet zápisů okolo 100 000. Při používání digitálních ID, která jsou platná většinou 1 rok je tento počet více než dostačující ;-)

Příště se již podíváme na požadavky nejdůležitější, tj. požadavky bezpečnostní.

Čipové karty a USB tokeny, aneb bezpečnější autentizace a šifrování (4) - bezpečnostní požadavky na tokeny I

Jak jsme si již naznačili, budeme se bavit o čipových kartách a USB tokenech, vůči kterým se autentizujeme znalostí hesla. HESLO (alfanumerické znaky) je vždy bezpečnější než pouhý PIN – Personál Identification Number (jenom číslice). Dále budu pro zjednodušení myslet „heslem" jak alfanumerické heslo, tak pouhý pin.

1. Heslo / PIN

Jak jsme si již naznačili, budeme se bavit o čipových kartách a USB tokenech, vůči kterým se autentizujeme znalostí hesla. **HESLO** (alfanumerické znaky) je vždy bezpečnější než pouhý**PIN** – Personal Identification Number (jenom číslice). Čtyř místný PIN má 104 = 10 000 kombinací, zatímco čtyřmístné heslo (znaky a-z a číslice) (26+10)4 » 1 680 000 kombinací. U osmi znakového hesla/pinu je pak rozdíl již o čtyři řády! Dále budu pro zjednodušení myslet „heslem" jak alfanumerické heslo, tak pouhý pin. Heslo je velmi důležité, neboť chrání náš token a informace v něm uložené při odcizení, či ztrátě.

2. Zablokování při opakovaně chybném zadání hesla

Je nutností, aby se token při několikanásobném špatném zadání hesla zablokoval! A to, ať je heslo jak chce dlouhé! Řekněme, že po 10 špatných pokusech o zadání hesla dojde k zablokování.

Co myslíme **zablokováním**? Základní možnosti jsou:

1. Automatické smazání všech informací uložených uvnitř.
2. Po zablokování lze token pouze ručně smazat pomocí utilit.
3. Pro odblokování se musí zadat další kód, většinou označovaný jako PUK.
   - po zadání kódu PUK má uživatel s heslem/pinem dalších 10 pokusů.
   - po zadání PUK může ten, kdo zná PUK kód nastavit nové heslo/pin.

Případy 1 a 2 se tedy týkají hlavně tokenů, ke kterým je pouze **jedno přístupové heslo** a po x špatných pokusech o zadání takovéhoto hesla dojde (hned, nebo následně) ke smazání obsahu tokenu. Takovéto čipové karty a USB tokeny lze vřele doporučit právě jako uložiště digitálních ID, šifrovacích klíčů atd. **Tokeny s jedním přístupovým heslem, jsou VŽDY z bezpečnostního hlediska lepší volbou!** Proč?

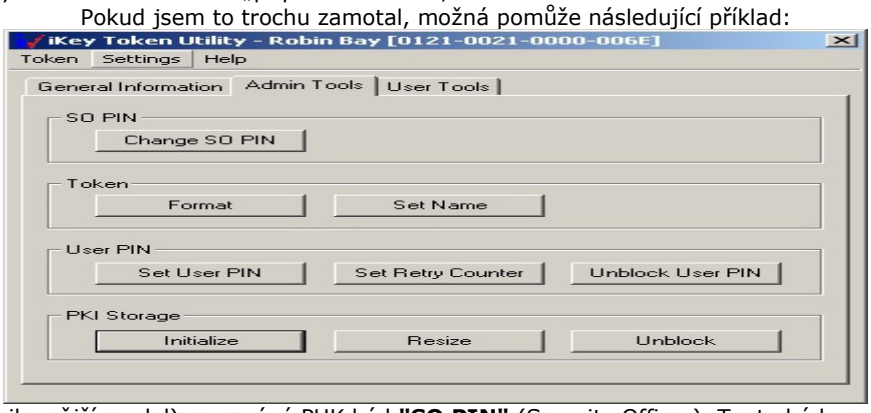
Pokud jde o případ 3, tak je třeba rozlišovat dvě různé situace. Buď zná všechna přístupová hesla tentýž člověk, nebo více lidí.

I.) Heslo/PIN a PUK kód vlastní tentýž člověk. Tento systém se používá na příklad u SIM karet v mobilních telefonech (nejde o nic jiného než o smart čip). Problém je v tom, že kód PUK uživatel buď vůbec nepoužije, nebo jen několikrát za celou dobu života řešení. Uživatelé si tedy kód PUK vůbec nepamatují a mají ho na nějakém kusu papírku "kdesi". Pokud jde o úroveň bezpečnosti, myslím, že to asi není třeba komentovat!

II.) PIN zná uživatel, zatímco PUK zná administrátor systému. Zde je velice dobré se zamyslet nad tím, co se stane po zadání kódu PUK. Dvě z nejpoužívanějších variant jsem již naznačil - možnost 3a a 3b. Možnost 3b lze použít v systémech, kde nevadí, že administrátor může nastavit uživatelovi nové heslo (na příklad: přihlašovací heslo do operačního systému). Jinak je ale většinou k smíchu, obzvláště je-li účel používání tokenů bezpečná úschova digitálních ID, či šifrovacích klíčů. Administrátor by se tak dostal k Vašim zašifrovaným datům (něco jako **EFS** ve Windows 2000 ;-), nebo by si přečetl Vaše šifrované emaily, digitálně za Vás podepisoval dokumenty, ... Možnost 3a je sice lepší, ale je třeba zvážit riziko, že bude moci administrátor zkoušet libovolné množství pokusů, i když mu to bude stěžovat ustavičné zadávání např. 9xPIN, jednou PUK, 9xPIN, ... Dalším problémem je u systémů s více přístupovými kódy fakt, že PIN je sice po několika špatných pokusech zablokován, ale vlastní PUK kód bývá této bezpečnostní pojistky zbaven!

Aby to nebylo tak snadné, tak je tu něco pro "vtipálky". Řekněme, že máte v tokenu šifrovací klíč k Vašim důležitým datům na HDD. Pokud by jste o tento šifrovací klíč přišli, přijdete také o všechna Vaše důležitá data na HDD (pokud nemáte šif. klíč zálohovaný). Jestliže máte zlomyslného kolegu, který se Vám chce za něco pomstít a zapomenete Váš token na stole, Váš "kolega" si token na chvilku půjčí a je to! Stačí, aby na příklad 10x stisknout enter na výzvu o zadání hesla, a máte velké problémy.

Existují i tokeny, kde po x špatných zadání dojde ke zničení předmětu, který se tak stane dále nepoužitelným. U všech ostatních systémů s jedním heslem je z ekonomických důvodů komukoli (nemusí znát žádné heslo) přístupná funkce smazaní obsahu tokenu! Takže Vašemu "kolegovi" stačí stisknout jednou tlačítko myši, nemusí ani mačkat 10x Enter :-(
Ale to už tak bývá, za vyšší bezpečnost vždy platíme menším pohodlím, větší cennou, atd. U tokenů s více hesly by zlomyslný vtipálek buď také token dokázal smazat, nebo, což je daleko horší, by měl i reálnou šanci se k obsahu dostat a zneužít ho! O to více nabývá na důležitosti tzv. „připoutání k tělu", kterému se budeme věnovat v dalších částech.
Pokud jsem to trochu zamotal, možná pomůže následující příklad:



U tokenů **iKey 1000** (nejlevnější model) se nazývá PUK kód **"SO PIN"** (Security Officer). Tento kód není omezen počtem zadání špatných pokusů! Uživatelův **"User PIN"** může administrátor nastavit, odblokovat ve smyslu umožnit několik dalších pokusů o jeho zadaní, ale také ho lze nastavit na novou hodnotu. Slouží tedy pro systémy, kde nevadí, že administrátor může nastavit nové heslo uživateli. Pro systémy, kde toto možné není (digitální podpis, šifrování dokumentů, ...) lze v tokenu vytvořit tzv. PKI oblast. Tato je chráněna heslem **"PKI",** které může Security Officer pouze odblokovat, ve smyslu umožnit dalších x pokusů o jeho zadání.
U tokenů iKey, řady 2000 je pouze jediné a tedy bezpečnější heslo. Po x špatných pokusech se token zablokuje a pak ho lze pouze inicializovat - tj. smazat vše uvnitř. Inicializaci může ale provést kdokoli, kdo má fyzický přístup k tokenu a nainstalovány utility. Tedy tokeny za vyšší cenu, ale bezpečnější = méně pohodlné.

Čipové karty a USB tokeny, aneb bezpečnější autentizace a šifrování (5) - bezpečnostní požadavky na tokeny II
Je otázka, jakou cestou (jak bezpečnou) putuje pin/heslo, které jsme zadali na klávesnici. U čipových karet, či USB tokenů, které mají přímo na sobě integrován snímač otisků prstů, je tato cesta bezpečná. Token také může mít hardwarovou podporu různých šifrovacích algoritmů a hash funkcí.

3. Cesta "tajemství" od zadání k porovnání

Je otázka, jakou cestou (jak bezpečnou) putuje pin/heslo, které jsme zadali na klávesnici. U čipových karet, či USB tokenů, které mají přímo na sobě integrován snímač otisků prstů, je tato cesta bezpečná. Naopak u USB tokenů a čipových karet, k nímž se autentizujeme "znalostí", musíme zadat heslo z klávesnice a to pak putuje do systému PC, kde může být odchyceno (na příklad rezidentním programem, který odchytává znaky přímo z portu klávesnice a ukládá je do souboru). Když si uvědomíme, kolikrát běžný uživatel stiskne klávesu na příklad během práce v internet exploreru...není prohledávání souboru se stisknutými klávesami zas až tak veliký problém. Další otázkou je pak to, zda heslo putuje zpět do čipové karty/usb tokenu, kde je vyhodnoceno (případ **procesorových tokenů**), nebo se porovnání děje softwarově (takto lze vyřešit přístup k **paměťovým tokenům** , které nelze pro většinu bezpečnostních systémů doporučit!!).
U čipových karet existuje možnost připojení numerické klávesnice ke čtečce nebo zakoupení klávesnice s integrovanou čtečkou. Zde potom "může" být zadaný kód vyhodnocen přímo čtečkou nebo klávesnicí. Zadané heslo, tak neputuje do systému. U USB tokenů jsem se s takovým řešením zatím nesetkal. Speciální klávesnice, která by při autentizaci neposílala znaky do systému, by totiž vzala USB tokenům jejich hlavní výhody: cenu a mobilitu. Systém s numerickou klávesnicí se navíc používá spíše tam, kde je uživatel v úplně cizím prostředí, takže hrozí reálné riziko "napíchnutí" zmíněné cesty (na příklad platební karty v obchodech).

4. Podpora šifrování v hardware

Token může mít hardwarovou podporu různých šifrovacích algoritmů a hash funkcí. Pro jednoduchost předpokládejme, že máme v tokenu symetrický klíč šifry **DES**. Pokud nebude mít token "**hardwarovou" podporu** algoritmu DES, znamená to, že při každém šifrování musí šifrovací klíč opustit token. Šifrovací klíč je zkopírován do počítače, kde je provedeno šifrování a pak je klíč ze systému smazán. Vzniká tak potencionální riziko, že díky nějaké chybě v software dodávanému k tokenu, může dojít k vyzrazení šifrovacího klíče. A to je přesně to, čemu chceme za každou cenu zabránit. Pokud bude mít token podporu přímo v hardware, šifrovací klíč token neopustí a bude neustále v bezpečí! Kromě hardwarové podpory DES se můžete setkat i s celou řadou dalších **symetrických šifer** (3DES, AES, ...). Podpora v hardware symetrických algoritmů ale není tak rozšířená, jako podpora algoritmů asymetrických.
Pro digitální podpis se využívají **asymetrické algoritmy** jako **RSA, DSA**... nejčastěji RSA s délkou klíče **512 nebo 1024 bitů. Kvalifikovaný certifikát** u „První certifikační autority" (vhodný i pro komunikaci se státní správou) používá privátní klíč délky právě 1024 bitů. Délky **RSA 2048 a 4096 bitů** se zatím využívají především pro „digitální podpis" serverů a certifikačních autorit samotných. Pokud bude mít čipová karta, či USB token nějakou hardwarovou podporu, tak většinou **RSA až 2048bitů.**

Čipové karty a USB tokeny, aneb bezpečnější autentizace a šifrování (6) - bezpečnostní požadavky na tokeny III
Běžným způsobem není možné zjistit, jak je zařízení fyzicky opravdu bezpečné. Jedinou možností je tedy spolehnout se na bezpečnostní certifikaci. V této oblasti existují dvě základní bezpečnostní certifikace: evropský ITSEC a americký FIPS. Další možností jsou určitě srovnávací testy, které jsou neocenitelnou pomůckou hlavně pro začínající uživatele.

5. Bezpečnostní certifikace

Běžným způsobem není možné zjistit, jak je zařízení fyzicky opravdu bezpečné. Výrobce Vám samozřejmě tvrdí, že je to SUPER! Na výstavě INVEX 2002 jsem na otázku: „V čem jste lepší (bezpečnější) než konkurence?" slyšel většinou odpovědi: **„Lepší hardwarová implementace."** :-))) Nelze očekávat, že Vám výrobce dodá detailní schéma zapojení uvnitř tokenu, aby jste se mohli přesvědčit! :-)

Jedinou možností je tedy spolehnout se na bezpečnostní certifikaci. V této oblasti existují dvě základní bezpečnostní certifikace: evropský ITSEC a americký FIPS.

I. Americká norma **FIPS** (vydaná NIST - National Institute of Standards and Technology)může mít úrovně 1 až 4. To, že dva tokeny splňují stejný "level" neznamená, že nabízejí stejnou bezpečnost. Zde **doporučuji si prohlédnout certifikát**, který Vám řekne, jakých výsledků dosahuje výrobek v jednotlivých kategoriích. Vybraný token s certifikací FIPS 140-1 level 2 totiž musí ve všech kategoriích splňovat úroveň "alespoň" 2. V některých kategoriích ale může být ještě bezpečnější! Další otázku, kterou doporučuji výrobci položit: **"Na co všechno se certifikace vztahuje?"** U USB tokenů se můžete setkat na příklad s "kousky", kde je certifikace na čip a firmware, některé mají certifikaci i na plastovou skořápku, která je vyplněna speciálním materiálem, takže při pokusu o rozdělání se skořápka rozlomí na mnoho malých částí a je tak jednoznačně evidentní (**tamper evident**) pokus o proniknutí...

Pokud token získá certifikaci, většinou je to **FIPS 140-1 level 2**. Tokeny (tedy myšleno čipové karty, či USB tokeny) s certifikací level 3 existují také, ale přirovnal bych je ke kulometu na komáry (i když určitě existují aplikace, kde je i tato bezpečnostní úroveň nutná). Kryptografických tokenů s certifikací **FIPS 140-1 level 3** a vyšší využívají například certifikační autority k ukládání privátních klíčů samotné autority. Nejedná se ale o čipové karty, či USB tokeny, nýbrž o jiné speciální zařízení (jako na příklad na obrázku). Tyto zařízení jsou konstruována tak, aby se při fyzickém pokusu o otevření uložené informace zničily (nejčastěji smazaly, v krajním případě se využívá i výbušnina) - tzv. **tamper resistant**.

Cryptoswift HSM - akcelerátor kryptografických operací s certifikací FIPS 140-1 level 3

II. Evropská norma **ITSEC** má úrovně E1 Basic až E6 High. Celkem 8 úrovní (úrovně 2 a 3 mají dva stupně). Čipové karty a USB tokeny dosahují většinou úrovně **E4 High**.

III. Další v Evropě uznávanou certifikací, je norma **CC (Common Criteria)**, nebo jinak: **EAL**. Tato norma je obecnější, než ITSEC a také novější. Vychází z ITSECu a dalších norem. Celkem má 7 úrovní (1..7), přičemž lze položit rovnítko mezi ITSEC E1 a EAL 2, atd. Čipové karty a USB tokeny s certifikací E4 High jsou tak zjednodušeně řečeno na úrovni **EAL 5**.

IV. Dalšími „certifikacemi" mohou být například : „**Entrust ready**", **OPSEC**, …. jde ve směs o certifikace „firemní". Vydávají je velké bezpečnostní firmy/společnosti, jako jsou Baltimore, Entrust, Check Point, RSA, …které tím naznačují, že konkrétní hardwarový token byl s jejich produktem odzkoušen a je plně funkční a „bezpečný". „Chytrý" výrobce bezpečnostních tokenů se chlubí, v kolika bezpečnostních produktech a od jakých firem je token podporován.

Za takováto loga se token rozhodně stydět nemusí ;-)

Další možností jsou určitě **srovnávací testy**, které jsou neocenitelnou pomůckou hlavně pro začínající uživatele. Zde bych však upozornil na **objektivnost**. Pokud se to dá, většinou zjistíte, že „výherce" klání čistě náhodou i sponzoroval finančně náročné testy (otestovat bezpečnostní řešení je trošku něco jiného, než test monitorů, či jiných běžných PC komponent). Navíc se mnohdy tzv. produkt „nedostane do uzávěrky". Pokud se dá patřičná "váha" těm "správným" parametrům, vždy vyhraje společnost, která test platí ;-) To je doufám jasné.

Byť se to nezdá, tak útoků na čipové karty existuje celá řada. Většinu z nich asi jen tak kdokoli provádět nemůže, ale zas tak nedostupné tyto útoky také nejsou. Útočit se dá na:

- **Software** čipové karty a jeho chyby
- Nějakým způsobem vyvolat **chybnou instrukci procesoru na čipu** – ozáření vhodným elektromagnetickým zářením, nečekanou změnou hodinového signálu, teploty….a čekat, že karta udělá nějakou chybu, které lze využít.
- Ledacos se dá zjistit také z času, který potřebuje procesor na šifrování (**timing attack**), z proudu, který karta při šifrování odebírá…Těmto útokům se říká „**útoky postranními kanály**".
- Existují i finančně náročné fyzické útoky, jako třeba mikrosondy, elektronový mikroskop, …

Bez certifikace si prostě nemůžete být jisti, že software a hardware je navržen správně a že karta odolá většině těchto útoků (hlavně těm „levnějším").

Čipové karty a USB tokeny, aneb bezpečnější autentizace a šifrování (7) - bezpečnostní požadavky na tokeny IV

V dalším pokračování našeho seriálu se podíváme na Import/Export klíčů, certifikátů a celých "ID" (otázka zní, jak se naše "klíče" do tokenu dostanou: možnosti jsou celkem dvě - buď je v tokenu vytvoříme, nebo je do tokenu importujeme) a podporu tokenů v oblasti programování.

6. Import/Export klíčů, certifikátů a celých "ID"

Otázka zní, jak se naše "klíče" do tokenu dostanou. Možnosti jsou celkem dvě. Buď je v tokenu vytvoříme, nebo je do tokenu importujeme.

Pokud má token podporu šifrování nějakého algoritmu v hardware, pak už je jen krůček k tomu, aby měl implementován i **náhodný generátor** a bylo tedy možné nejen šifrovat v tokenu, ale vlastní šifrovací klíč v tokenu vytvořit. Pokud tedy chcete co největší bezpečí Vašeho šifrovacího klíče, či privátního klíče pro digitální podpis, žádejte po tokenu tyto vlastnosti:

- **Klíč nelze vyexportovat z tokenu ven.**
- **Klíč je používán na tokenu a při šifrování/podepisování neputuje do systému**
- **Klíč/e lze na tokenu vytvořit**

Řekněme, že chcete vytvořit pár veřejný-privátní klíč pro digitální podpis. Co se bude dít po vytvoření (certifikáty, atd.) nechme teď stranou.

Existují asi tyto základní možnosti:

- RSA pár **vytvoříte přímo na tokenu** - jednoznačně nejbezpečnější. Ale i tato možnost má svojí vadu. Vadou není bezpečnost, ale to, že pokud pár na tokenu vytvoříte, velmi pravděpodobně (lze jen doporučit) nebudete mít možnost si tento pár klíčů zálohovat (vyexportovat z tokenu) a to může být problém při ztrátě či krádeži tokenu!

- RSA pár **vytvoříte pomocí dodávaného softwaru k tokenu** . Zde dojde k softwarovému generování, software za Vás klíč do tokenu nahraje a "možná" Vám před smazáním klíče z paměti RAM umožní jej zálohovat do souboru. Méně bezpečné, ale pokud je PC, na kterém generování probíhá "důvěryhodné", není to většinou žádný veliký problém.
- RSA pár **vytvoříte v nějakém software** , který umožňuje zálohování a pak jej v podobě souboru importujete pomocí dodávaných utilit do tokenu.

Pozn. add 1. Problém ztráty tokenu, ve kterém máte nezálohovaný pár asymetrické šifry RSA tkví v tom, že si sice přečtete Vámi digitálně podepsané emailové zprávy, ale už nebudete schopni si přečíst zprávy, které Vám byly zaslány a byly šifrované.
Pozn. add 3. Možnost vytvořit pár klíčů tímto způsobem máte na příklad při žádosti o "digitální identitu" přes internet. Při výběru "Typ klíče" na www.ica.cz (testovací certifikát) máte možnost zvolit "Microsoft Base Cryptographic Provider". Tato možnost odpovídá tomu, že v operačním systému Windows bude vytvořen pár klíčů. Ten pak lze exportovat do souboru "**.pfx**" a pomocí něho pár klíčů importovat do tokenu.
Soubory s příponou **.pfx** jsou soubory, které splňují standard **PKCS#12** (po "Microsoft" způsobu ;-) Normálně mají soubory tohoto standardu příponu "**.p12**" Dodržování tohoto standardu je velmi důležité, protože řada bezpečnostních systémů umožňuje vyměňovat klíče i celé "digitální identity" právě pomocí těchto souborů.
Pro import samotných certifikátů slouží většinou soubory **.cer, .der, .crt**. Doporučuji zjistit pomocí jakých souborů lze digitální ID, certifikáty, šifrovací klíče, či další "objekty" do tokenu importovat.

7. PKCS#11 versus MS CAPI

Velmi důležitá je i podpora tokenů v oblasti programování. Zde se setkáváme nejčastěji s **Microsoft Cryptographic API (MS CAPI)** nebo **Criptoki (standard PKCS#11)**. Pokud vytvoří programátor svoji aplikaci tak, aby fungovala podle standardu PKCS#11, měla by fungovat téměř s jakýmkoli tokenem, který tento standard splňuje. I naprostý laik by se tak měl dívat, zda token splňuje standard PKCS#11, neboť tím má "téměř" zaručeno, že bude token fungovat nejen v utilitách dodávaných k tokenu, ale i v celé řadě dalších systémů a aplikací. Téměř znamená, že je přesto radno si u výrobce prověřit, zda je token v dané aplikaci podporován. Počet aplikací, podporujících tokeny podle PKCS#11, se každým dnem zvyšuje. Entrust, Lotus Notes, PGP a mnoho dalších systémů podporuje řadu čipových karet a USB tokenů od různých výrobců jen díky tomuto standardu. Aniž by jste programovali, poptejte se... Pokud jste přímo programátoři, je výhoda standardu jasná - lze dodat zákazníkovi token, jaký si přeje a Vy nebudete závislí na jednom dodavateli tokenů.
Více informací o standardech PKCS se dočtete v češtině na stránkách archivu článků T.Rosy a V.Klímy (články vyšly v časopisu CHIP r.2000 a 2001), nebo stránkách společnosti RSA Security. Další standardy PKCS se zabývají vlastní šifrou RSA (PKCS#1), vytvářením žádostí o certifikát (PKCS#10), vytvářením šifrovacího klíče z hesla, atd.

Čipové karty a USB tokeny, aneb bezpečnější autentizace a šifrování (8) - bezpečnostní požadavky na tokeny V

Robin Bay Tutoriály 3. září 2003

Předmět můžeme někde zapomenout, ztratit, nebo nám může být odcizen. Jak jsme si již řekli, může "záškodník" kartu smazat, zablokovat nebo může zkoušet uhádnout heslo. Nelze zapomenout ani na případ, kdy útočník odpozoruje PIN. I samotná ztráta tokenu může být veliký problém, pokud jsme si šifrovací klíč uvnitř nezazálohovali.

8. Připoutání k tělu

Této „drobnosti" bychom měli věnovat více pozornosti, než se jí v mnohých případech dostává.
Předmět můžeme někde zapomenout, ztratit, nebo nám může být odcizen. Jak jsme si již řekli, může "záškodník" kartu smazat, zablokovat nebo může zkoušet uhádnout heslo. Nelze zapomenout ani na případ, kdy útočník odpozoruje PIN. I samotná ztráta tokenu může být veliký problém, pokud jsme si šifrovací klíč uvnitř nezazálohovali. Musíme tedy nějak zajistit, aby uživatel token nikde nezapomenul, neztratil, ani aby mu nebyl odcizen.
Předmět lze zapomenout většinou:

- **V místnosti, kde je používán.** Ideální proto je, pokud se uživatel bez předmětu „nedostane" ven z objektu, kde

USB token - Jedna z výborných možností, jak zamezit ztrátě, či zapomenutí předmětu

předmět používá. Čipové karty využívané zároveň pro vstup do objektu nebo USB tokeny na svazku klíčů, které uživatel potřebuje k zamknutí místnosti/objektu, jsou naprosto ideální.

- **V kapse oblečení.** Člověk je tvor líný a tak nemusí vždy dát čipovou kartu k ostatním dokladům, do peněženky nebo prostě tam, kam patří. Zvláště pokud ji používá vícekrát za den. Proto se čipové karty často ocitnou v kapse oblečení. Sako s čipovou kartou přehozenou přes židli se tak může stát snadným cílem. U předmětů, které lze připnout na svazek klíčů je tato možnost minimální. Klíče si totiž hlídá každý člověk již od věku, kdy mu je rodiče dají na krk. Možná Vám to zní to legračně, ale funguje to! Nebo jste snad někdy v poslední době ztratili své klíče?

Pokud se v prostředí s vysokými požadavky na bezpečnost použijí čipové karty, vyvrtá se do karty dírka, provlékne se šňůrka a šup na krk. Z vlastní zkušenosti mohu potvrdit, že USB token jsem zatím nikde nezapomněl ani neztratil. Čipovou kartu jsem již párkrát nechal právě v oblečení, které k mému štěstí zůstalo jenom doma. Legrační ale nebyl nutný návrat domů, protože bez karty jsem jakoby neexistoval...
Připoutání k tělu se využívá také pro donucení uživatelů k tomu, aby se při sebemenším vzdálení od PC odhlásili, nebo tzv. "zamknuli" stanici. Pokud se dá uživateli USB token na klíče, tak při odchodu na oběd si vezme klíče s sebou, zvláště tehdy, pokud se bez nich k vytouženému obědu nedostane, tj. má na nich klíče od auta, kanceláře, budovy, bezkontaktní token pro docházkový systém, …. Nejlepší, pokud jsou na svazku i klíče od uživatelova osobního majetku, potom si dává opravdu veliký pozor a token je opravdu v bezpečí ;-)

Čipové karty a USB tokeny, aneb bezpečnější autentizace a šifrování (9) - ceny a závěrečné srovnání

Posledním důležitým parametrem, ve kterém se čipové karty a USB tokeny liší, je cena. Pokud chcete začít používat opravdu bezpečný digitální podpis a přihlašování do operačního systému, pak za hardware dáte přibližně 3000,- Kč. Levnější tokeny (tedy bez certifikace s méně bezpečnostními funkcemi) mohou vyjít klidně i o polovinu levněji.

Cena

Posledním důležitým parametrem, ve kterém se čipové karty a USB tokeny liší, je cena. Pokud budeme uvažovat, že chcete začít používat opravdu bezpečný digitální podpis a přihlašování do operačního systému, pak Vás "příslušná" čipová karta bude stát něco kolem 1000,- Kč. Čtečka čipových karet, bez které se neobejdete, zhruba 2000,- Tedy jen za hardware dáte přibližně 3000,- Kč. Za tuto cenu už ale mluvíme o poměrně "bezpečném" hardware i s FIPS 140-1 level 2 certifikací. Stejný USB token (myšleno se stejným čipem, firmware a se stejnou FIPS certifikací) seženete ve směs o pár korun levněji. Jenže! Pokud se ale budeme bavit o levnějších tokenech (tedy bez certifikace s méně bezpečnostními funkcemi) může Vás USB token vyjít klidně i o polovinu levněji, než řešení se stejně funkční čipovou kartou! (a to právě kvůli vysoké ceně čtečky čipových karet, kterou u USB tokenů nepotřebujete).

Abych uvedl konkrétní příklad, tak na webových stránkách "jistá" firma nabízí USB token iKey 2032 FIPS za 2990,- Kč. Ta samá firma nabízí čipovou kartu Datakey Model 330 (kde je naprosto! stejný čip jako ve zmiňovaném USB tokenu) za 890,- Kč. Vtip je ale ve čtečce za 2100,- Kč (sériový/USB port). Takže zmiňovaná řešení vyjdou na stejnou cenu.

Pokud ale zvolíme levnější model USB tokenu iKey2000 (který nemá FIPS certifikaci a má méně paměti), tak ten u dané firmy vychází na 1890,- Kč. No a za tuhle cenu už možná seženete čtečku čipových karet, ale bez vlastní (tokenu ikey2000 odpovídající) čipové karty. Nemluvě o ještě levnějších modelech USB tokenů řady iKey 1000.

Cenově se čipové karty vyplatí hlavně tehdy, jedná-li se o využívání na principu "počítačové učebny". Tedy využívá-li jeden počítač více lidí. Pak se ušetří za čtečky (třeba jen 30 čteček na 200 uživatelů).

Srovnání

Shrňme si tedy hlavní oblasti ve kterých se "obecně" čipové karty a USB tokeny liší.

Vlastnost tokenů	Čip. karty	USB tokeny
Odolnost konektorů (záleží na garanci výrobce)		+
Mobilita (USB tokeny nepotřebují čtečku)		+++
Víceúčelovost, personifikace (foto, magnetický proužek, bezkontaktní čip, …)	+++	
Při použití speciálního pin padu ke čtečce, heslo nemusí putovat do systému		
Připoutání k tělu		+++++
Cena 1 uživatel/PC		++
Cena více uživatelů/PC	+	

Čím více znamének "+", tím si myslím, že má daný token výhodu oproti tomu druhému.