

Praktické využití multitechnologických karet

V minulém čísle SecurityWorldu byly popsány jednotlivé typy elektronické identifikace kartou – slučování do jediné multitechnologické karty. Ted' se zaměříme na praktické využití tohoto řešení.

KAREL PIŠTĚK

Instalace přístupového systému spočívá v zavedení jak softwarové, tak hardwarové části. U prvně jmenované se jedná většinou o balík, ve kterém jsou zpracovávána data ze vstupních terminálů, jež jsou na základě těchto informací dále ovládány.

Zde závisí délka instalace na příslušném vybavení hardwarem a také standardním softwarem, například zavedení SQL databáze a sy-



HID karta Crescendo

stému na serveru a následně pak na jednotlivých stanicích – v závislosti na architektuře. Pro středně složitý a jinak připravený systém může být instalace přístupového systému provedena i během jediného dne.

Distribuce příslušných karet je pak otázkou jejich dostupnosti v rámci jejich výroby a aktivace – zavedení do systému a předání jejich uživateli.

Vlastní kartu lze vyrobit a aktivovat do jedné minuty (jde o potisk příslušnými identifikačními údaji spolu s grafickým návrhem). Přitom lze na kartě provést čtení a zápis v rámci jejího pořízování v jediném procesu: zavést její sériové číslo do databáze, zapsat data/zaklíčovat bezkontaktní část, nahrát certifikát do kontaktní části, nahrát data do magnetického proužku a vytisknout její grafický design a třeba i čárový kód.

Nahrávání certifikátu se může protáhnout až na několik minut, zvláště vyhledává-li se například v centrální databázi, a též jeho velikost může ovlivnit dobu jeho nahrávání.

U bezkontaktních karet například návrhový software CardFive od portugalské firmy Nfive pro tisk a práci s kartou dovoluje použít prostředky pro grafický návrh karty, propojení s externí databází přes ODBC rozhraní, a má i mnoho dalších funkcí. Navíc nabízí i jednu velice užitečnou a praktickou možnost: volání externí aplikace, která řídí zpracování – zápis/čtení karty a vstup např. pomocí klíčů v průběhu její přípravy. Externí aplikace přitom musí zajistit vedení karty – například v tiskárně karet vedení do vestavěného kodéru (čtečky/zapisovačky) – stejně tak jako vedení karty do tiskové stanice po jejím nakódování, atp.

Použití multitechnologické karty

Možností použití jediné multitechnologické karty je nezměrně. Lze ji nasadit současně v aplikacích a situacích, jako jsou:

- docházkové a přístupové systémy,
- biometrické systémy (zápis otisku prstu přímo do karty),
- otevření zámku,
- fyzický přístup do dveří,
- logický vstup do počítače (IT systému),
- vjezd na parkoviště, do garáží apod.,
- v dopravních prostředcích pro odečítání jízdného,
- ve zdravotnictví pro identifikaci pacienta/lékaře,
- při použití kopírky,
- pro nákup v automatu,
- použití elektronické peněženky pro čerpání služeb v rámci např. vysokoškolského kampu,
- a v mnoha dalších aplikacích.

Pro systém Windows (ale i další) vyvinula firma HID Global program, který s využitím karty Crescendo zaručuje maximální zabezpečení a jednoduchost ověření například identity zaměstnance.

INZERCE

Sovte

Technologie pro autorizovaný přístup k Vaším datům a majetku

potisk, kódování a laminace ID plastových karet, čtečky kontaktních a bezkontaktních karet, identifikační karty, navigo™ a CRESCENDO™ řešení pro logický a fyzický přístup



Identifikační | klubové | docházkové | věrnostní | debetní | bankovní | jízdenky



VÝHRADNÍ ZASTOUPENÍ | AUTORIZOVANÝ SERVIS | ID SECURITY SYSTÉMY | AUTENTIZACE

SOVTE, Hodkovičká 8, Praha 4, tel. : 244 472 725, 244 471 787 | fax: 241 470 814 | e-mail: sovte@sovte.cz

www.sovte.cz

NaviGo autentizuje

V dnešní době zatím používá jen velmi málo organizací dvoustupňové ověřování identity. Program naviGo řeší tento základní problém tak, že přímo „připojuje“ systém Windows ke kartám s technologií, která na trhu převládá – HID kartám pro řízení přístupu.

Samotný operační systém Windows byl totiž navržen tak, že podporuje pouze dva způsoby ověřování: jméno uživatele/heslo a používání kontaktní Smart karty. Program naviGo rozšiřuje tyto dva způsoby o možnost používání HID karet s technologiemi typu Proximity a iClass.

V současné době více než 200 milionů uživatelů počítačů může používat karty, které již mají právě pro fyzický přístup, i k dvoustupňovému ověřování. Tento fakt sám o sobě významně zmenšuje nepříjemné bariéry týkající se přizpůsobení počátečních nákladů na spolehlivé ověřování a nepřizpůsobivosti rozmístění/neflexibilní rozmístění.

Použitím programu naviGo lze získat velký náskok, neboť ostatní řešení pro přihlašování uživatele nemohou používat již existující prostředky pro práci s kartami. Navíc kombinací programu naviGo s HID kartami Crescendo (viz SecurityWorld 2/2009) nebudou ztraceny žádné již existující procesy identifikace – zůstanou stále k dispozici všechny nástroje pro podporu špičkové infrastruktury s veřejným klíčem (PKI).

Program naviGo umožní převést celou organizaci na dvoustupňové ověřování pomocí již existujících identifikačních karet pro přístup. Nejpřitažlivější je skutečnost, že program naviGo může podporovat sou-



časně všechny technologie karet, takže je možné karty zaměňovat a sladit tak, aby pro organizaci bylo možno navrhnout nejhodnější bezpečnostní program.

Čtečka Cardman 5325 CL USB Prox pro čtení jak bezkontaktních karet HID Prox, tak čtení kontaktních karet (třeba Crescendo), je jednoduše připojena k PC pomocí USB rozhraní. V okně Windows pouze přibudou kromě standardních ikonek „User Name and Password“ a „Insert a Smart card (PKI)“ dvě další ikonky: „Contactless Logon“ a „Emergency Access“.

Příklad ISO norem pro komunikaci s kartou s RFID čipem

Pro nejdůležitější RFID karty platí normy ISO uvedené v tabulce. Přitom je důležité i to, že níže uvedené standardy platí pouze pro komunikaci. Čtení dat a konverze např. na Wiegand, C&D (Clock&Data), RS485 jsou specifické pro čtečky a výrobce.

Jednotlivé typy neznámějších bezkontaktních karet na frekvenci 13,56 MHz uvedené v tabulce splňují uvedené části normy. Například norma ISO 14443A-4 definuje jednak tvar amplitudové křivky typu A, jednak část 4 definuje transmisní protokol pro DesFire karty. V porovnání splňují tedy třeba karty Mifare normu typu A, zatímco karty iClass normu typu B. Amplituda radiofrekvenčního signálu u typu A klesá až na 5 % úroveň, zatímco u typu B jen asi na 80 % (zjednodušeně řečeno). Karty iClass mají například definován větší dosah – až do 1m.

Normy pro karty RFID

RF rozhraní	iClass	Mifare	DesFire
ISO 14443A		část 1–2–3	část 1–2–3–4
ISO 14443B	část 1–2		
ISO 15693	část 1–2–3		
Komunikační rychlost	424 Kb/s nebo 26 Kb/s	106 Kb/s	424 Kb/s
Operační vzdálenost	až do 100 cm	až do 10 cm	až do 7 cm

část 1 – fyzikální charakteristiky; část 2 – radiofrekvenční výkon a signálová interference; část 3 – inicializace a antikolize + aktivací protokol; část 4 – transmisní protokol

Využití biometrie

Biometrické přístupové systémy využívají pro jednoznačné určení totožnosti osoby částí jejího těla, tzv. tělových identifikátorů. K ověřovacímu procesu neboli verifikaci dochází zpravidla teprve po zadání PIN kódu. Co se nejčastěji kromě otisků prstů využívá?

- **Verifikace duhovky** – podobně jako otisky prstů, i oční duhovka je u každého člověka jedinečná.
- **Verifikace dlaně** – je založena na měření fyzikálních charakteristik ruky a prstů z pohledu třídimenzionální perspektivy.
- **Verifikace hlasu** – elektricky je provedena analýza digitálního „otisku“ lidského hlasu.

Využívání biometrických prvků zažívá v současnosti druhý boom. První byl zhruba před osmi lety, ale používaná technologie měla dost slabých míst, ukázalo se, že například dvě až tři procenta lidí nebyla identifikovatelná pomocí biometrických prvků z nejrůznějších důvodů. Rovněž se dal otisk prstu přenést na papír a snímač tak přelstít.

Dnes se tyto systémy vylepšují a kombinují – například otisk prstu musí mít nejen požadovanou strukturu, ale také i teplotu lidského těla. Sleduje a ověřuje se třeba i hlas, oční duhovka apod. Spolu s vložením karty a vlastním otiskem se ještě zadává na čtecím zařízení PIN.

Systémy jsou dnes propracované, je celá škála jejich vyhodnocování, a používají se spíše jako doplněk jiných kartových a čipových systémů, zejména tam, kde je třeba zajistit násobné zabezpečení v důležitých a tajných provozech, tam, kde není možné, aby vstoupila například osoba se zapůjčenou kartou.

Závěrem

Problematika čipových karet je velice složitá, nicméně v současnosti se jejich zavedením zabývá stále více firem a státních institucí. Často je jejich zavedení naprosto nezbytné, například pro ověřování pro komunikaci přes internet, pro přístup do určitých systémů a souborů pomocí kontaktní čipové karty s certifikátem a identifikací.

Velmi důležitou oblastí je i fyzický přístup do budov, areálů, hlídaných místností atd. Nemalý význam má proto jednak postupně nenásilné a cenově přístupné zavádění multitechnologických karet, kde přechod k systémům s vyšší bezpečností nebo jejich zavádění je relativně jednoduché, stejně tak jako používání této jediné karty pro různé systémy a aplikace.

Autor je ředitelem firmy Sovte.

Technologickým partnerem a sponzorem tohoto příspěvku je společnost Sovte.