INFORMAČNÍ SYSTÉMY VE VEŘEJNÉ SPRÁVĚ

doc. RNDr. Ing. Roman Šperka, Ph.D.

INFORMAČNÍ SYSTÉMY VE VEŘEJNÉ SPRÁVĚ

IDENTIFIKACE, AUTENTIZACE, AUTORIZACE

Identifikace, autentizace, autorizace

Identifikace

- přiřazení známé veličiny v rámci systému neznámé entitě, takže ta se stane systému známou
- známá veličina se nazývá identifikátorem (často označovaným ID), což je ve většině případů jméno nebo nějaké kódové označení
- aby nedocházelo ke komplikacím, je požadováno, aby identifikátor byl jedinečný alespoň v rámci daného systému.

Autentizace

- stvrzuje pravost (autenticitu) identifikace
- u autentizace osob se jedná o ověření, zda se jedná opravdu hlásicí se osobu, autentizace objektů zpravidla znamená potvrzení jejich původu

Autorizace

- přiřazuje identifikované a autorizované osobě práva, kterými disponuje v daném systému
- v praxi se jedná o přiřazení zařízení, přístupu k datům, rozsah funkcionality poskytované služby, práva vykonávat určité činnost v rámci systému atd.
- většinou se to děje na základě přidělování registrovaných rolí přihlašovanému uživateli

Způsoby autentizace osob

na základě znalosti

- vstupních kódů, popř. postupů (textový login, textové heslo, PIN, posloupnost operací atd.);

na základě vlastnictví identifikačního předmětu

- karta, čárový kód, hardwarový klíč identifikační doklad apod.

na základě toho, že člověk má určitou jedinečnou vlastnost

- biometrika (biologické vlastností uživatele, např. otisky prstů, sítnice apod.)

Znalostní autentizace

Zadávání hesla, PINu

- pravidla pro tvorbu a ochranu hesla
- ke změně hesla je nutné přistoupit, má-li přihlášený uživatel podezření nebo jistotu jeho prozrazení
- hesla společná skupinám uživatelů (málo bezpečná)

Výzva – odpověď

- je založena na tom, že žadatel potvrdí vhodnou odpovědí znalost reakce na výzvu
- bezpečnost metody je založena na tom, že výzva je vysílána pouze jednou a mění se
- výzva a odpověď jsou spojeny, je vytvořen jejich „otisk“, který je zaslán k ověření
- v ověřovacím systému je postupováno stejně a v případě shody otisků je povolen vstup do systému.

Autentizace nulové znalosti (v angl. Zero-Knowledge)

- žadatel prokazuje pouze znalost hesla, ale nevyzrazuje žádnou jeho část
- jedna strana transakce přesvědčuje s určitou pravděpodobností druhou stranu, že má určitou znalost bez toho, že by prozradila, co zná
- dokazovatel (ten, kdo se autentizuje) je schopný dokázat platnost nějaké skutečnosti právě tehdy, když je tato skutečnost pravdivá
- ověřovatel (ten, kdo vyžaduje autentizaci) na rozdíl od výše zmíněných metod heslo žadatele nezná
- metoda zachovává anonymitu uživatele

Identifikační prvky

- systémy čárových kódů;
- systémy karet;
- systémy radiofrekvenční identifikace;
- hardwarové klíče;
- elektronické klíče.

Čárové kódy

- k dispozici je cca 50 druhů čárových kódů, navržených pro nejrůznější aplikace
- často posuzován jen vnější efekt čárového kódu (urychlení operací a odstranění chyb obsluhy pokladny)
- dobře navržený a správně aplikovaný IS však poskytuje daleko cennější služby, tj. informace
  - např. přesný a okamžitý přehled o struktuře a množství prodaného zboží, o pohybu osob apod.
- značení s využitím čárového kódu je nejpropracovanější formou automatické identifikace vůbec
- u nás nejznámější je soustava značení kódem EAN, která znamená jednoznačnou identifikaci jakéhokoliv zboží, které se objeví ve světové obchodní síti, rychle se rozšiřuje i značení sdružených obalových jednotek

Karty

- Magnetické snímací karty
  - např. platební karty, docházkové a objednávkové systémy, kopírovací karty atd.
  - základ karty tvoří magnetický pásek nesoucí identifikační údaje o majiteli karty.
  - bezpečnost těchto karet je ale malá vzhledem k tomu, že není relativně žádný technický problém pořídit si kopii magnetického proužku.

Karty

- Čipové inteligentní karty
  - jsou vlastně o miniaturní počítač velikosti kreditní karty, který spolehlivě autentizuje uživatele a chrání data při velmi nízkých nákladech na pořízení a udržování
  - mikročip může pracovat jako pouhá paměť typu EPROM (například telefonní karty), nebo jako plnohodnotný mikroprocesor.
  - mikroprocesor pak poskytuje celou řadu služeb, jako je autentizace pomocí uloženého hesla, či kryptografické operace.
  - tyto karty obsahují několik základních prvků zachování bezpečnosti:
    - dvoufaktorová autentizace uživatele, přístup do sítě je umožněn, pouze pokud se vloží karta do čtečky a zadá číslo PIN,
    - bezpečné uchování digitálních certifikátů na přenosném a programovatelném mediu, karta umožňuje vygenerovat a uložit držitelův soukromý klíč a digitální certifikáty se zabezpečením proti neautorizovanému přístupu nebo kopírování,
    - odpovědnost uživatele za elektronické transakce, lze s jistotou určit, kdo a které elektronické operace provádí, uživatelé tak jsou plně zodpovědní za svoje aktivity online,
    - strategie single sign-on (jediného přihlášení), zhuštění přihlašovací procedury do jediné metody řeší problém velkého počtu uživatelských jmen hesel bez ztráty na stupni zabezpečení.

Systémy radiofrekvenční identifikace

- karty nebo přívěsky, opatřené integrovaným obvodem reagujícím na elektromagnetické a rádiové vlny
- mají vlastní paměť, z níž lze data číst i je do ní rádiem ukládat.
- používají se na osobní identifikační karty a identifikační přívěsky pro nejrůznější pohyblivé objekty jako jsou automobily, vagóny, kontejnery a podobně.
- umožňuje speciálním snímacím zařízením přečíst číslo (kód) zboží, resp. obalové jednotky
- nositelem kódu je subminiaturní elektronický čip (transpondér), který vysílá příslušný kód na vzdálenost několika centimetrů do svého okolí, je tvořen elektronickým obvodem, který obsahuje přijímací/vysílací anténu, nabíjecí kondenzátor a paměť obsahují naprogramované údaje
- potřebnou energii většinou čipu dodá čtecí zařízení (vysílač/snímač)
- konstrukce čipu pak umožňuje jeho pevné zabudování do tělesa obalové jednotky, kde je zcela chráněn před vlivy prostředí
- životnost moderních radiofrekvenčních čipů je prakticky neomezená a v této aplikaci zdaleka přesahuje životnost obalové jednotky.

Hardwarový klíč

- zařízení, které se připojí na počítač nebo jiné zařízení prostřednictvím paralelního nebo sériového portu, USB apod.
- lze ho použít v lokálním nebo síťovém provedení
- lokální klíč musí být připojen přímo na počítači, síťový klíč je připojen většinou na serveru
- některé umožňují přístup k paměti v klíči, který je chráněn pomocí PIN
- nenalezne-li aplikace klíč, nespustí se nebo spustí pouze omezený modul (informace, demonstrační režim atd.).
- podle úrovně zabezpečení, které nám poskytují je můžeme rozdělit:
  - tokeny pouze s pamětí, jsou obdobou mechanických klíčů, paměť může obsahovat jednoznačný identifikační řetězec,
  - tokeny udržující hesla, po zadání jednoduchého uživatelského hesla vydají určený kvalitní klíč, který udržují,
  - tokeny s logikou, umí zpracovávat jednoduché podněty typu vydej následující klíč, vydej cyklickou sekvenci klíčů, může mít omezen počet použití, pomocí těchto tokenů lze realizovat systém s one-time hesly, k ochraně programů, přístupům
  - k nejrůznějším placeným službám apod.
- jsou nejpoužívanější ochranou pro komerční software vyšších cenových kategorií, ochraně aplikací již nainstalovaných na počítači a dat

Elektronický klíč

- plní funkce autentizace a certifikace (jednoznačné potvrzení správnosti předávaných dat) za pomoci šifrování.
- mobilní elektronický klíč se používá prostřednictvím mobilního telefonu
- umožňuje to technologie GSM SIM Toolkit, kterou je dnes vybavena většina přístrojů
- přístup k mobilnímu elektronickému klíči v telefonu je chráněn speciálním osobním identifikačním číslem (BPIN), veškerá komunikace s bankou probíhá šifrovaně

PIN kalkulátor

- technicky autonomní zařízení s kódovanou čipovou sadou, která generuje autentizační kód
- kalkulátor pracuje samostatně bez jakéhokoli přímého propojení s počítačem nebo bankou
- na základě vnitřních hodin PIN kalkulátoru (datum a čas) je generován v časovém intervalu cca 30 s autentizační kód
- pro každý tento časový interval a PIN kalkulátor je vygenerovaný kód jiný
- ověření správnosti kódu probíhá v zabezpečeném prostředí banky.
- použití SSL umožňuje autentizaci založenou na asymetrické kryptografii (typ 3), konkrétně X.509 certifikátech
- uživatel obdrží osobní certifikát od certifikační autority
- s tímto certifikátem se pak může autentizovat v rámci skupiny serverů, které této certifikační autoritě důvěřují
- uživatel může bez rizika použít jeden certifikát pro autentizaci na více místech (web serverech)
- na rozdíl od jména/hesla, které je možno si lehce zapamatovat, certifikát nemusí mít uživatel vždy po ruce
- osobní certifikáty obsahují základní údaje o uživateli a jsou tedy velmi vhodné pro "instantní registraci", tj. uživatel je ušetřen zdlouhavého vyplňování formulářů, protože základní údaje jsou převzaty právě přímo z certifikátu

Biometrika

- metoda identifikace podle biologických vlastností uživatele
- mezi tyto metody patří:
  - otisky prstů;
  - oční sítnice;
  - oční duhovka;
  - tvář;
  - hlas;
  - podpis;
  - geometrie ruky.

Otisky prstů

- systémy poměrně pokročilé také v oblasti verifikace přístupů do různých prostorů a k počítačům a sítím
- snímače otisků využívají nejčastěji elektrický, optický, ultrazvukový, tepelný a tlakový princip snímání:

Křemíkové snímače

- využívající měření elektrické kapacity pomocí matice malých kondenzátorů, tvořených prvky křemíkového čipu a přiloženým prstem

Optické snímače

- využívají změny odrazu světla v místech dotyku papilárních čar se snímačem

Ultrazvukové snímače

- využívají různou zvukovou vodivostí papilárních linií a vzduchu v mezipapilárních mezerách

Tepelný a tlakový princip

- je využíván zejména jako doplněk jiných principů pro ověřování „živosti“ prstů (snímání jejich teploty a pulsace krve).

Oko

Sítnice

- využívá unikátnosti rozložení krevních cév a vlásečnic v oční sítnici (retina) jednotlivých osob.
- pro sejmutí tohoto rozložení musí být použity speciální snímače, využívající obvykle laserové paprsky, což není příjemné
- sejmutý obraz však obsahuje dostatek informací pro jednoznačnou identifikaci osob.

Duhovka

- využívá unikátnosti duhovky lidského oka (iris)
- dle udávaných údajů je pravděpodobnost existence dvou shodných duhovek nesrovnatelně menší než u otisků prstů
- vzorec duhovky je téměř neměnný od jednoho roku věku a mění se jen při některých nemocech, rovněž není závislý na rozšíření zornice.

- snímání je prováděno kamerou, uloženou za zrcadlem
- při snímání systém nejprve zaregistruje drobné mimoděčné pohyby pro ověření „živosti“ oka, pak proběhne zaostření sejmutí a vyhodnocení.

Rozpoznávání obličeje

- využívají programově simulovaných neuronálních sítí a prvků umělé inteligence
- při videoanalýze napodobují algoritmy lidského mozku, tím je dodávána novým systémům schopnost „naučit“ se podobu jednotlivých osob a následně ji porovnávat se snímaným obrazem
- technologie používá jako základ pro biometrickou identifikaci obličejovou charakteristiku., pro zakódování obličeje jsou používány speciální algoritmy
- matematické transformace zajistí převod do indexu, který může být uložen ve standardní databázi pro velmi rychlé následné prohledávání.
- k hlavním výhodám patří nenáročnost na uživatele a přirozený způsob verifikace a identifikace odpovídající lidským postupům
- u špičkových systémů lze dosáhnout velmi vysoké bezpečnosti a spolehlivosti bez možnosti oklamání

Verifikace lidského hlasu

- identifikace osoby pomocí rozšířené analýzy digitálního „otisku hlasu“
- tvar hlasivek, ústní dutiny, jazyka a zubů způsobují, že rezonance vokálního traktu je u různých osob dostatečně odlišná
- jednou z nejúspěšnějších technik je porovnávání vzorků pomocí analýzy signálů řeči
  - testovaný subjekt přečte systémem náhodně zvolenou frázi, sejmutá zvuková stopa je kmitočtově omezena (nejčastěji 3kHz) a je proveden rozbor zvuku na základě původu jednotlivých složek zvuku v činnosti hlasového aparátu a jazykových pravidel
  - výsledek je komprimován na vzorek velikosti 1 až 2 kB a porovnán se srovnávacím vzorkem. Verifikace hlasu se používá zejména k řízení přístupu do informačních systémů prostřednictvím telefonu

Podpis

- osoba se musí podepsat na speciální podložku pomocí speciálního pera
- systém ověřuje podpis osoby na základě porovnání s uloženým podpisovým vzorem, který popisuje, jak byl popis napsán.
- není důležitá jen podoba podpisu či tvar písmen, ale důraz je kladen na dynamiku podpisu, provedení tahů, sílu, kterou tlačíme při psaní na podložku, rychlost psaní, změny tlaku, zrychlení v jednotlivých částech, celkový průběh zrychlení, zarovnání jednotlivých částí podpisu, celková rychlost, celková dráha a doba pohybu pera na a nad papírem apod.
- to vše podává jednoznačnou charakteristiku libovolného podpisu
- ze získaných hodnot je opět vytvořen vzorek, který je porovnán se srovnávacím vzorkem
- do této skupiny lze zařadit i metody využívající sledování rytmu psaní na klávesnici.

Tvar ruky

- měření fyzikálních charakteristik ruky a prstů z hlediska třídimensionální perspektivy
- zkoumá se délka a šířka dlaně a jednotlivých prstů, boční profil ruky apod.
- tvar ruky je snímán speciálním skenerem, který produkuje třírozměrnou fotografii a redukuje tato data do malého vzorku
- speciální systémy mohou využívat identifikaci podle tvaru chodidla, způsobu chůze atd.

Doklady

- doklady, jejichž primární funkcí je určení totožnosti majitele
  - např. občanský průkaz apod.;
- doklady, pomocí kterých majitel prokazuje určité oprávnění
  - např. řidičský průkaz apod.

Strojově čitelné cestovní doklady

- specifikace jsou stanoveny v dokumentu 9303 Mezinárodní organizace pro civilní letectví (ICAO)
- podle těchto norem se strana s osobními údaji dělí na dvě zóny:

Zóna vizuální kontroly – Visual Inspection Zone,

- obsahující označení dokladu, fotografii obličeje držitele, osobní údaje a údaje týkající se vydání dokladu a jeho platnosti;

Strojově čitelná zóna – Machine Readable Zone,

- obsahuje některé z informací obsažených v zóně vizuální kontroly v podobě alfanumerických znaků a symbolu „<”, a to ve dvou či ve třech řádcích
  - tuto posloupnost znaků lze přečíst pomocí čtecího zařízení a usnadnit tak kontroly cestovních dokladů.

Strojově čitelné zóny - formáty

ID1 (86 x 54 mm)

- 3 řádky, na každém 30 znaků, umístění na zadní straně (verso) dokladu;

ID2 (105 x 74 mm)

- 2 řádky, na každém 36 znaků, umístění ve spodní části strany s osobními údaji či ve spodní části víza;

ID3 (125 x 88 mm)

- 2 řádky, na každém 44 znaků, umístění ve spodní části strany s osobními údaji.

Strojově čitelné údaje

- typ dokladu,
- kód vydávajícího státu,
- příjmení jméno, popřípadě jména občana,
- číslo cestovního dokladu,
- státní občanství,
- datum narození,
- pohlaví,
- doba platnosti dokladu,
- rodné číslo
- kontrolní číslice, které jsou číselným vyjádřením vybraných údajů ve strojově čitelné zóně.

Nosič dat (čip)

- uchování údajů o
  - zobrazení obličeje,
  - otiscích prstů rukou,
  - údajích zpracovaných na datové stránce cestovního pasu
  - dalších bezpečnostních prvcích stanovených přímo použitelnými právními předpisy Evropských společenství
  - obsahuje digitálně zpracovanou fotografii občana a jeho podpisu
- uvedené biometrické údaje lze použít výlučně pro ověření totožnosti občana pomocí osobních údajů zapsaných v cestovním dokladu a prostřednictvím technického zařízení umožňuje srovnání aktuálně zobrazených biometrických údajů občana (zobrazení obličeje, otisky prstů) s údaji zpracovanými v nosiči dat cestovního dokladu
- k žádosti o vydání cestovního pasu se nepředkládá fotografie, úředník pořídí fotografii žadatele přímo na oddělení cestovních dokladů
- elektronické doklady se obvykle využívá rádio-frekvenční rozhraní

Zabezpečení dokladů

- prvky zamezujícími jejich falzifikaci
- ochrany před
  - kopírováním
  - neoprávněným čtením dat z čipu
- mechanismus autentizace je realizován jako digitální podpis datových souborů označovaných DG1 až DG19, což jsou soubory nesoucí aplikační data pasu
- na českých pasech jsou využívány:
  - DG1 – kopie strojově čitelné zóny pasu;
  - DG2 - biometrická fotografie držitele
  - DG3 - otisk palce;
  - DG15 - veřejný klíč aktivní autentizace

Identifikační doklady

- dvě hlavní kategorie identifikačních dokladů:
  - cestovní dokumenty;
  - národní průkazy totožnosti.
- všechny, bez ohledu na využívané technologie musí být chráněny proti padělání a krádežím (usurpování) identity
- různost předpisů a zvyklostí nejen ve světě, ale i uvnitř Evropské unie. Jde především o to, že:
  - v některých zemích je národní průkaz totožnosti dobrovolný, někde není využíván vůbec a jeho funkci plní pas;
  - na území jednotlivých států platí zároveň několik typů dokumentů, založených na různých technologiích

Identifikační doklady

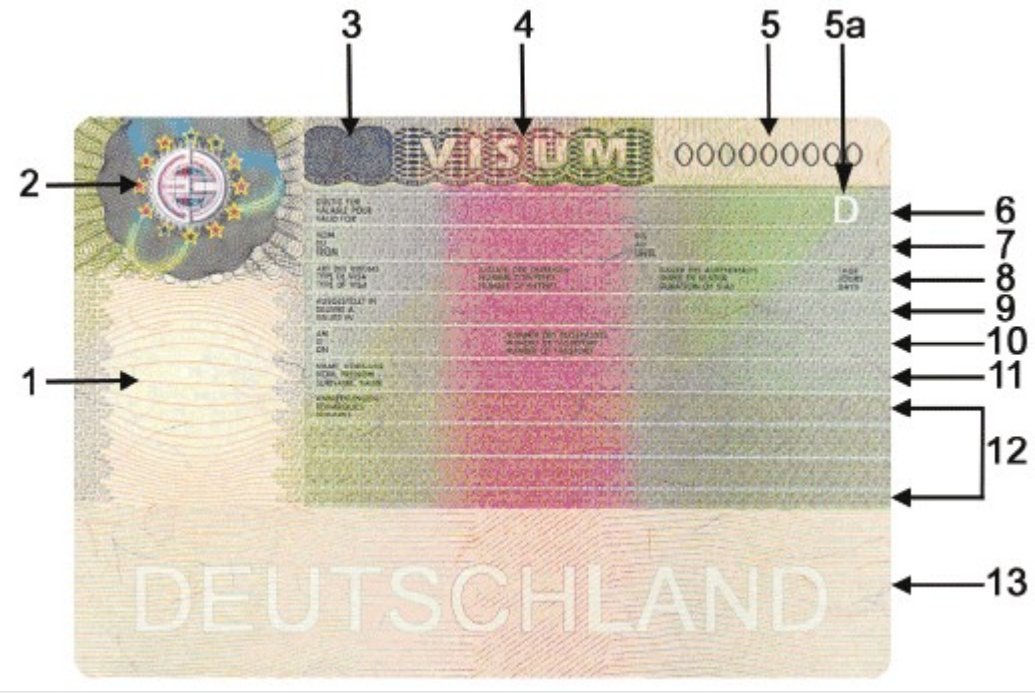
- dvě hlavní kategorie identifikačních dokladů:
  - cestovní dokumenty;
  - národní průkazy totožnosti.
- všechny, bez ohledu na využívané technologie musí být chráněny proti padělání a krádežím (usurpování) identity
- různost předpisů a zvyklostí nejen ve světě, ale i uvnitř Evropské unie. Jde především o to, že:
  - v některých zemích je národní průkaz totožnosti dobrovolný, někde není využíván vůbec a jeho funkci plní pas;
  - na území jednotlivých států platí zároveň několik typů dokumentů, založených na různých technologiích

Občanský průkaz

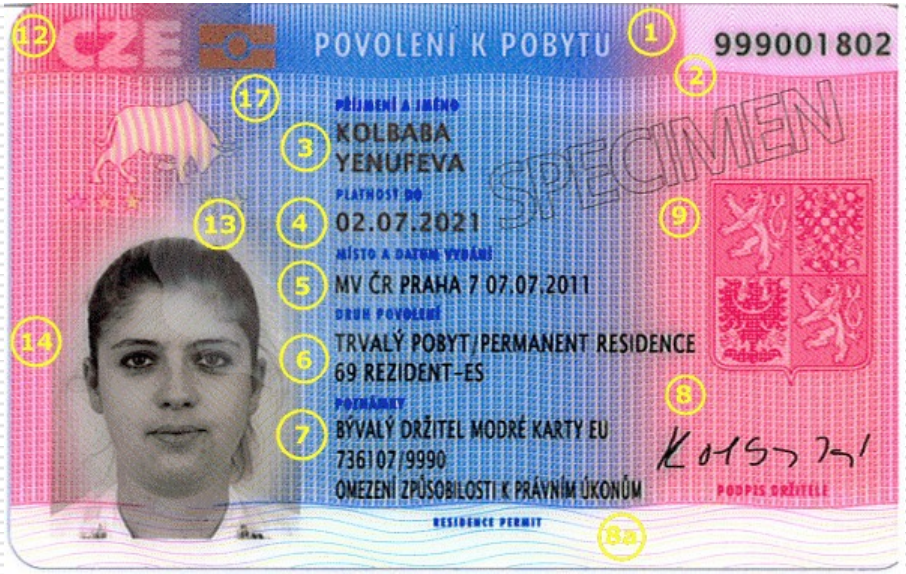
- na zadní straně je umístěn kontaktní elektronický čip, do kterého lze nahrát elektronický podpis (podle § 17b odst. 1 zákona číslo 227/2000 Sb., o elektronickém podpisu, ve znění pozdějších předpisů).

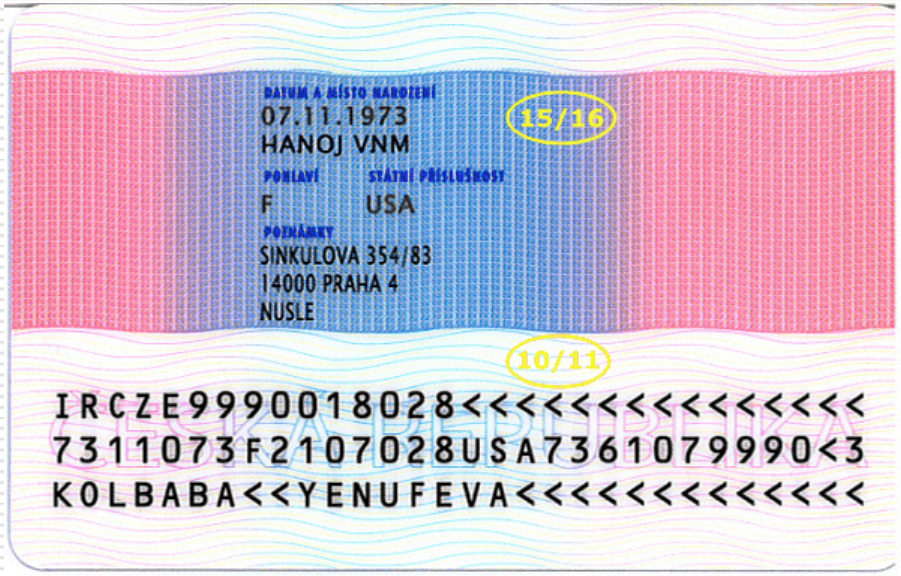
Cestovní doklady s biometrickými prvky

Vízum



Průkaz o povolení k pobytu pro cizince z třetích zemí





Řidičský průkaz

Děkuji za pozornost.

Otázky?