BIOMETRIE A RFID

BIOMETICKÉ METODY V BEZPEČNOSTNÍ PRAXI

ÚVOD

Nárok na uchovávání velkého množství dat

Nároky na vyšší zabezpečení

BIOMETRIE

(nahrazování běžných hesel biometrickým prvkem „unikátnost každého z nás“)

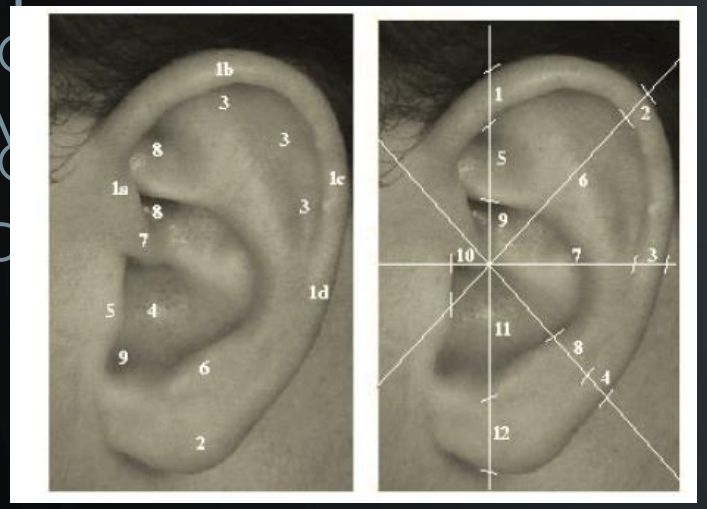
ÚVOD

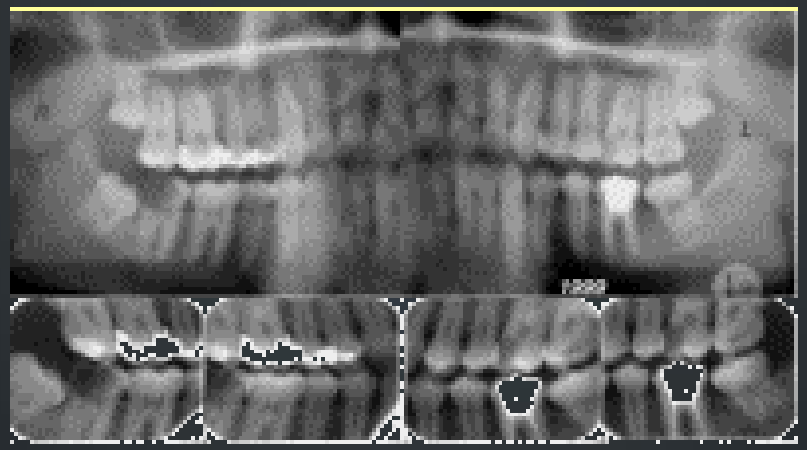
- Kniha „Biometrie a identita člověka“ – identita osoby je definována jako „nezbytná podmínka bytí každé konkrétní osoby“...(Rak Roman, 2008, str. 37).
- Pojem „biometrie“ vychází z řeckého „bio“ – život a „metric“ porovnávat
- Bohatá historie

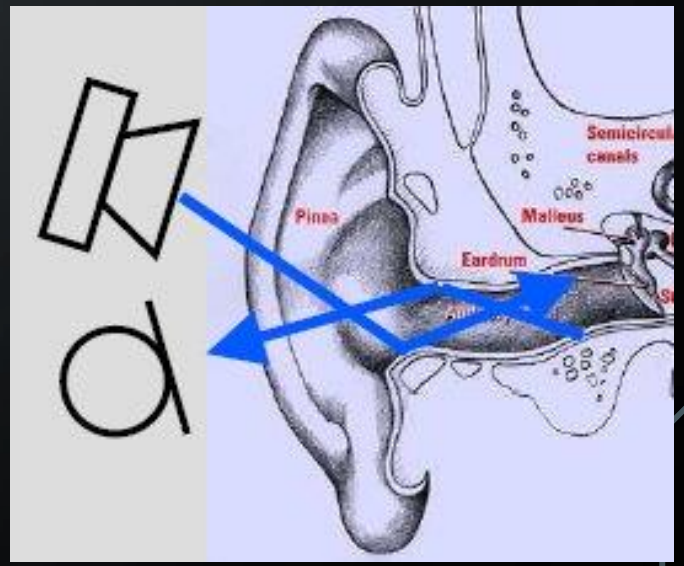
HISTORIE

- V jeskyni, jejíž stáří je odhadováno minimálně 31 000 let, jsou stěny ozdobeny malbami, o kterých se předpokládá, že byly vytvořeny prehistorickým člověkem. Kolem těchto maleb můžeme nalézt několik otisků dlaně. Tyto otisky dlaně jsou považovány za jakýsi druh podpisu majitele.
- Záznamy o používání otisku prstu jako prostředku identifikace osob se datují až k roku 500 před n.l. Byly to Babylonské obchodní záznamy, které byly zaznamenávány do jílových desek spolu s otiskem prstu.
- Joao de Barros, španělský průzkumník a spisovatel, napsal o raných čínských obchodnících, kteří používali otisk prstu na uzavření obchodních transakcí. Čínští rodiče používali otisk prstu i na rozlišování jednoho dítěte od druhého.
- V Egyptských dějinách je záznam o obchodnících rozlišovaných podle jejich „obchodních knížek“, které obsahovaly záznamy o jejich transakcích, aby bylo možné rozlišení mezi důvěryhodnými obchodníky a novými obchodníky na trhu.


onbao.com


1b
3
3
8
1a
1c
3
8
7
1d
5
4
9
6
2
1
2
5
6
9
10
7
3
11
8
4
12




Pinna
Malleus
Eardrum

VYUŽITÍ BIOMETRIE

- Charakterizování člověka – identifikace jednotlivců
- Sledování biometrických znaků pro další zpracování (behaviorální biometrie)

lidský mozek zpracovává intuitivně

KONTROLA OPRÁVNĚNÍ OSOBY

- **Heslem** – Posloupnost znaků. Nejnižší stupně zabezpečení. Lze se jich zmocnit a jsou přenositelná.
- **Předmětem** – Vlastnictvím tokenu s pamětí, heslem. Lze se jich zmocnit a jsou přenositelné. Může dojít k vyzrazení hesla a zapůjčení tokenu.
- **Biometricky** – Využívá tělesných znaků. Nejvyšší stupeň zabezpečení. Jsou nepřenositelné. Rychlá, pohodlná a přesná metoda
- **Kombinace uvedených metod**

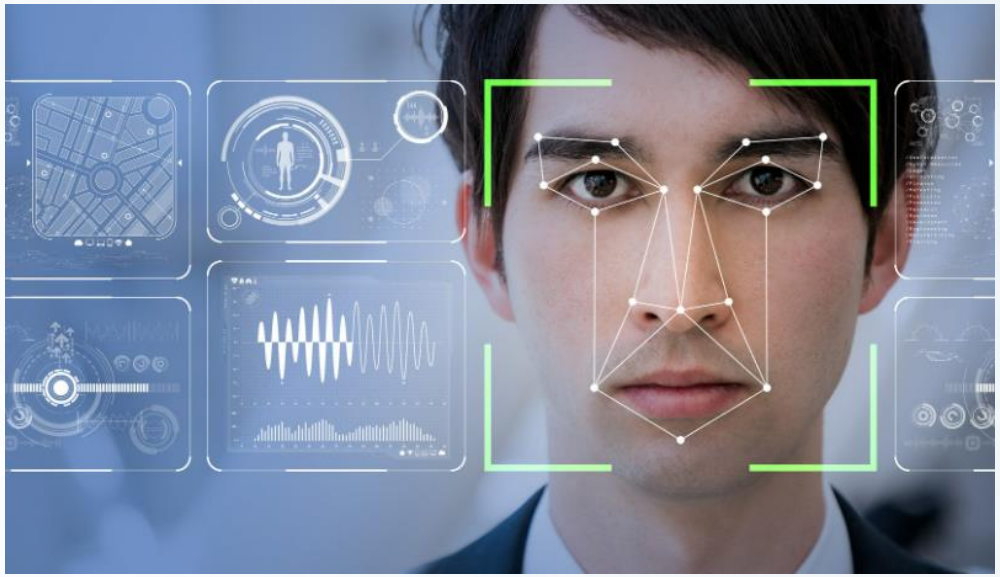
POJMY

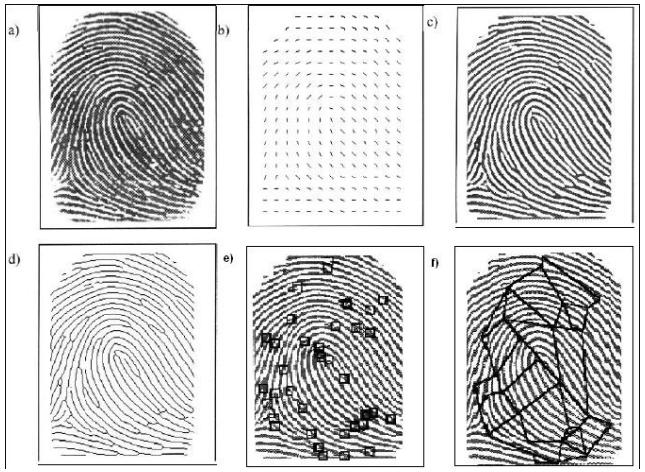
- Identifikace – určení totožnosti (porovnání se všemi vzorky). Vzor se porovnává se všemi známými šablonami a hledá se shoda (podobnost).
- Verifikace – ověření totožnosti (srovnání se vzorkem zapsaným k dané osobě). Vzor např. na ID kartě se porovnává pouze s osobní šablonou dané osoby.
- Autentizace – rozpoznávání, přidělení statutu (oprávněný/neoprávněný).

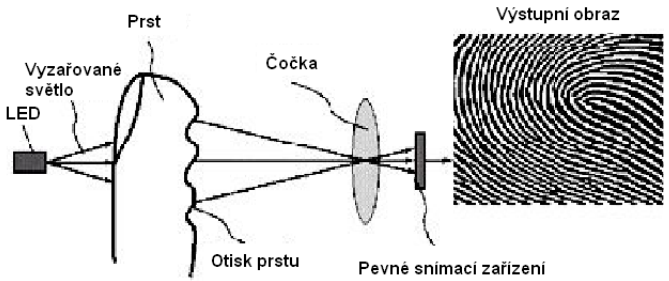
BIOMETRIE

- Vědní obor zabývající se zkoumáním živých organismů (bio), především člověka, a měřením (metric) jeho biologických (anatomických a fyziologických) vlastností a chováním.
  - Znaky získané geneticky (genotypické),
  - Znaky získané ve vývoji embrya (randotypické),
  - Znaky chování získané učením, (behaviorální)

- Biometrický údaj je citlivým osobním údajem
- Zákon č. 101/2000 Sb., o ochraně osobních údajů ve znění pozdějších změn (fyziologická, psychická, kulturní, ekonomická, nebo sociální identita).



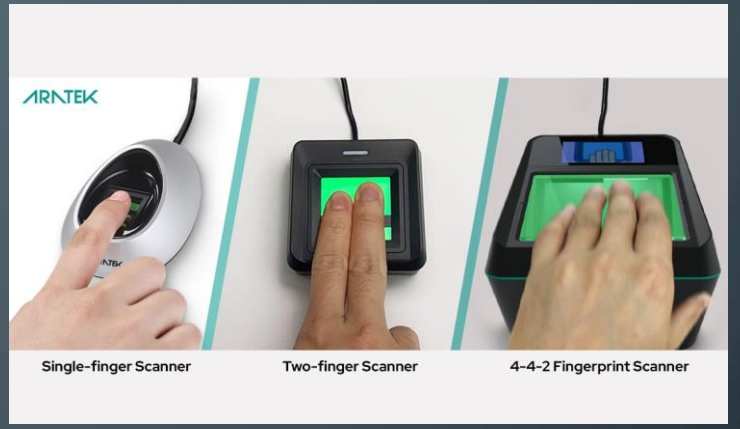


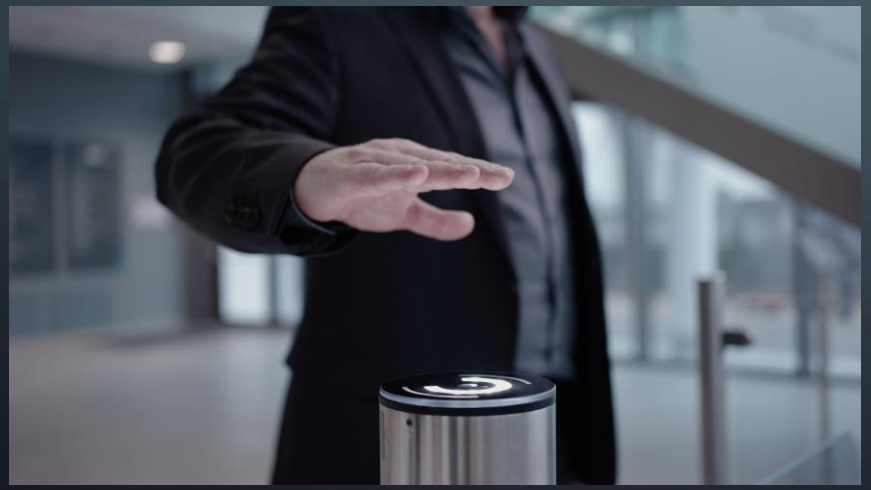


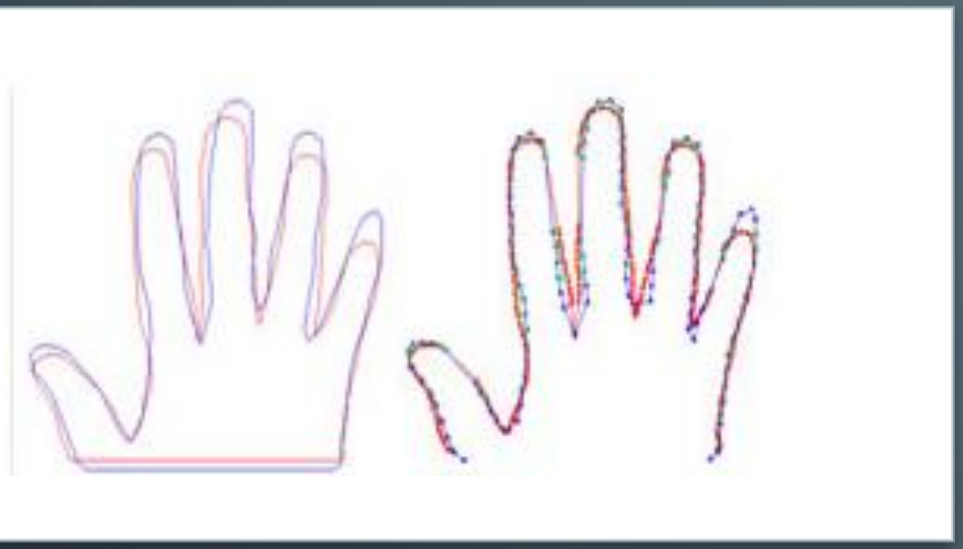
OTISK PRSTU

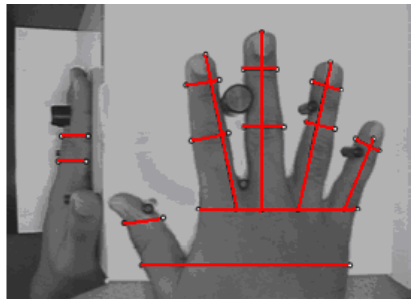
- Obrazce papilárních linií na vnější straně prstů rukou, nohou a dlaní
- Pravděpodobnost shodnosti otisků dvou žijících osob je odhadována na 6*10-8
  - Tlakové snímače
  - Rádiové snímače
  - Teplotní senzory
  - Ultrazvukové snímače
  - Optické senzory
  - Elektro-optické snímače
  - Kapacitní snímače
- Reakční čas: 0,2 - 1 sekunda
- Spolehlivost : vysoká

OTISK PRSTU


ARANTEK
Single-finger Scanner
Two-finger Scanner
4-4-2 Fingerprint Scanner



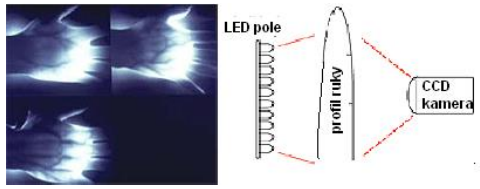


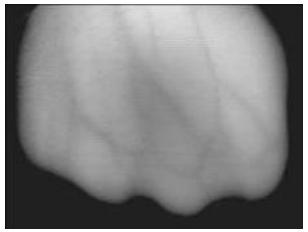


GEOMETRIE RUKY

- Od roku 1985, rok 1996 Olympijská vesnice Atlanta.
- Nevyužívá se otisku prstů (ruky), ale měření bodů a velikosti úseček
- Problém s otlaky (bižutérie, prstýnky)

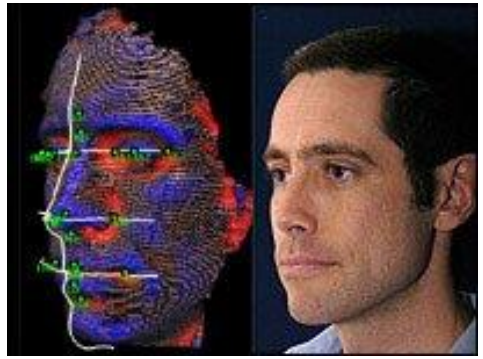
GEOMETRIE RUKY

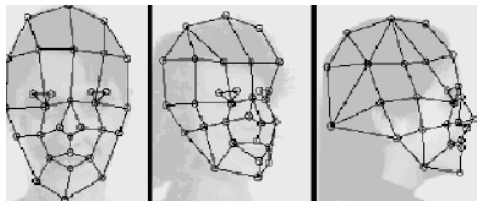




KREVNÍ ŘEČIŠTĚ ŽIL ZÁPĚSTÍ

- Aplikace přibližně od roku 2000
- Síť cév uvnitř ruky není viditelná a snímání vyžaduje, aby byla ruka živá, tekla v ní teplá krev, obtížné napodobení.

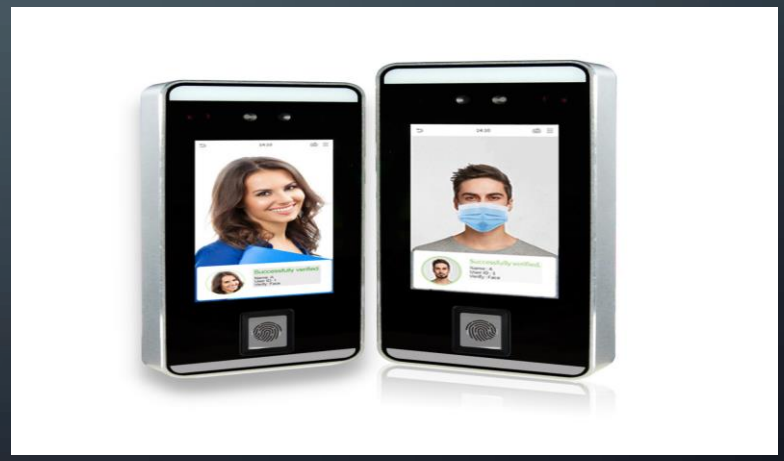


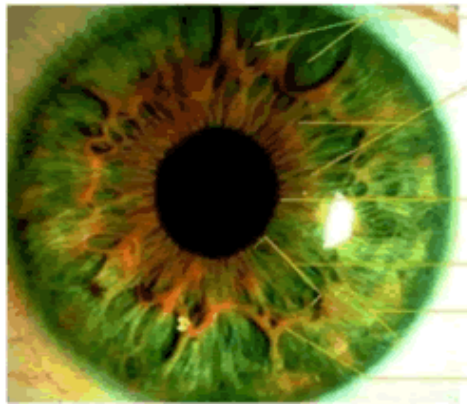


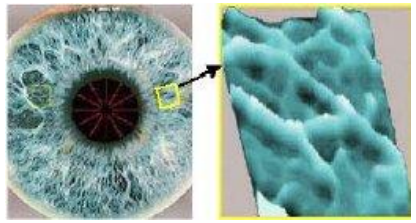
GEOMETRIE TVÁŘE

- Srovnávání obrazu sejmutého kamerou s obrazem, který je uložen v centrální databázi
- K identifikaci slouží tvar obličeje a poloha opticky významných míst na tváři.
- Základní 2D geometrie změří vzdálenost mezi nosem, ústy, očima a jinými rysy (nedostatečné pověření)
- Pokročilá 3 geometrie zaznamená obličej pomocí laserových snímačů a není závislá na okolním prostředí nebo poloze.
- Ideální v kombinaci s jinou metodou, jako je snímání duhovky, tepelný obraz tváře a jiné

GEOMETRIE TVÁŘE

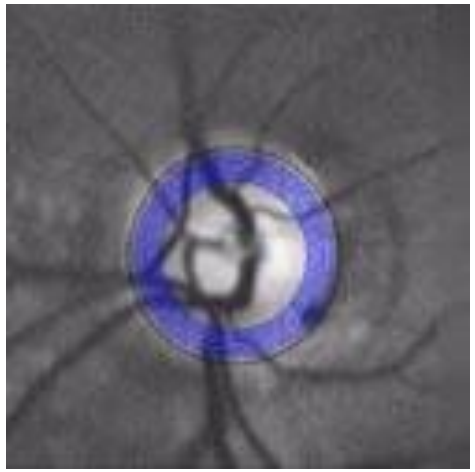


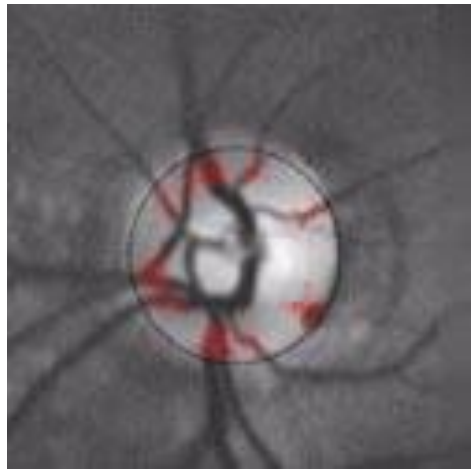


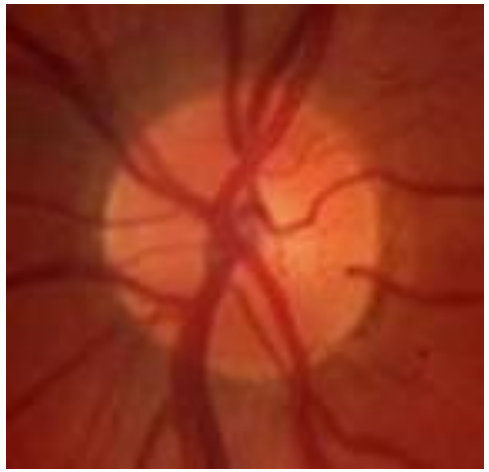


DUHOVKA OKA

- Oční duhovka je nejpřesnější biometrickou šablonou pro ověření
- Kromě reakce duhovky na světlo není ovlivněna jinými faktory
- Neměnný orgán, žádné dva vzory se neshodují (levé/pravé oko)
- Problém s řasami, čočkami, odrazy, scanovací zařízení je drahé, kód duhovky může být zpětně zrekonstruován k vytvoření šablony
- Reakční čas: 2 – 4s



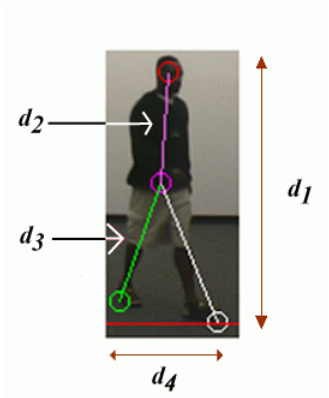


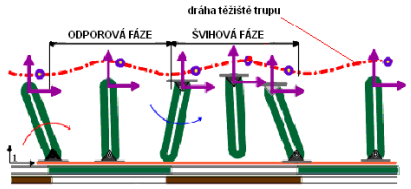


SÍTNICE OKA

- Struktury cév na pozadí lidského oka.
- Je složena z velkého množství nervových buněk.
- Reakční čas: 1,5 až 4 s

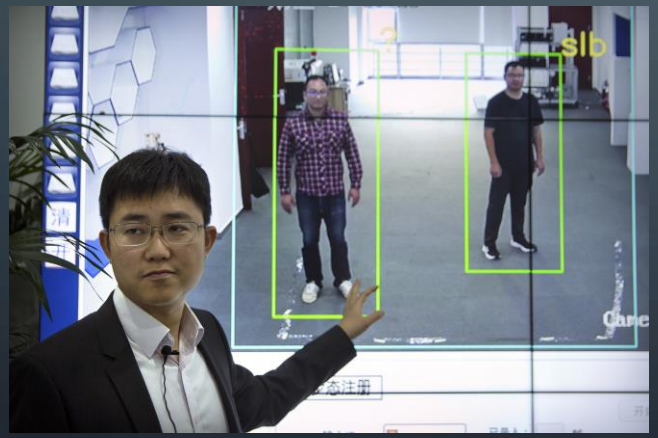
BEHAVIOMETRIKA

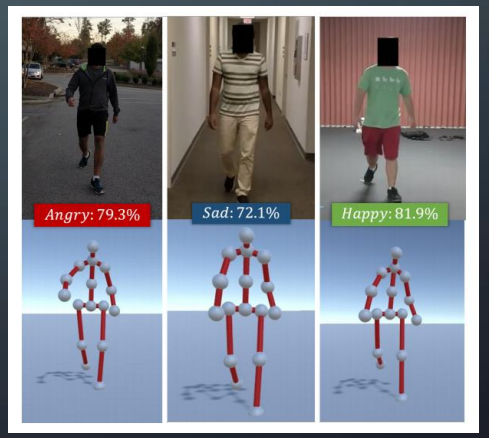




- Vlastností osoby lze identifikovat na velkou vzdálenost.
- Mění se v čase.
  - Styl psaní na klávesnici (dynamická biometrie) – četnost úderů, jejich rytmika.
  - Autorizace pomocí akustické charakteristiky hlasu.
  - Bipedální dynamika, rytmus a stereotyp těžiště.
  - Dynamika rukopisu
  - Pohyb rtu…..atd.

BEHAVIOMETRIKA (GAIT RECO)





DALŠÍ METODY …

- Styl psaní na klávesnici (dynamická biometrie) – četnost úderů, jejich rytmika.
- Autorizace pomocí akustické charakteristiky hlasu.
- Bipedální dynamika, rytmus a stereotyp těžiště.
- Dynamika rukopisu
- Pohyb rtů
- Rozpoznávání uší (detektor Optophone od ART Techniques)
- Rozpoznávání tělesných pachů (sensory vyvinuté Cambridge University) jsou schopny zachytit a analyzovat čichové vůně lidského těla z nepotících se částí těla jako je ruka, které jsou potom extrahovány biometrickým systémem a použity jako šablona a autentizační prostředky.)
- DNA

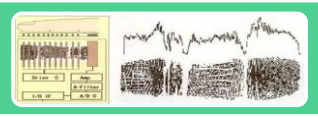
Biometrie ucha (boltec a zvukový kanálek)

Morfometrické vztahy v geometrii ušního boltce. Otisk. Rozložení teploty na ušním boltci

Spektroskopie kůže

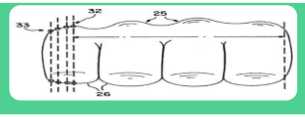
Vrstvy mají odlišnou tloušťku. Vlnová délka světla se láme a odráží v jiné vrstvě pokožky

Krevní řečiště dlaně



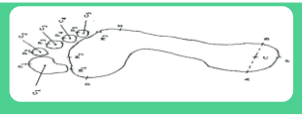
Vrásnění článků prstů a kloubů prstů

1998, Elektrostatické kapacitní reaktance měření vrásek za klouby prstu



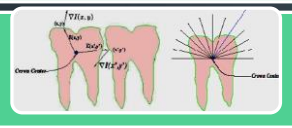
Tvary článku prstu a pěsti

35 parametrů



Plantogram

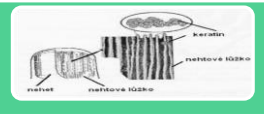
Vnitřní stavba chodidla, Kresba papilárních linií. Kombinace 38 rozměrů.



Biometrické vlastností zubů a čelisti

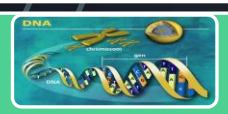
Pach

30 chemických sloučenin vytváří profil. Senzory, zvířata



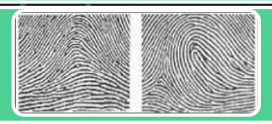
Podélné rýhování nehtů

K identifikaci je využito keratinu v prostoru mezi nehtem a nehtovým lůžkem



DNA

DNA odlišná , výjimka jednovaječných dvojčat.Zdlouhavá procedura.



Porometrie

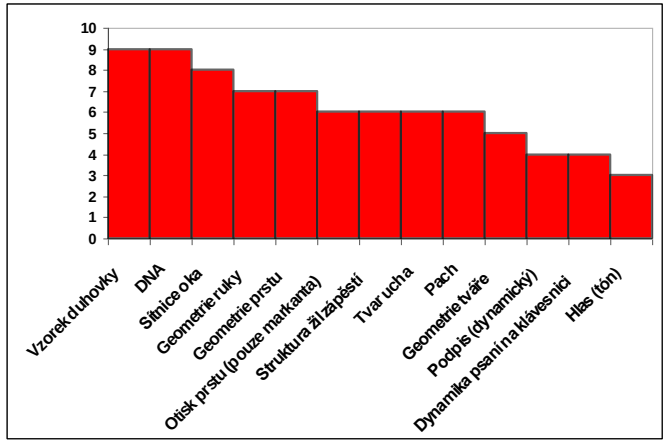
Vzhled a lokalizace kožních pórů,

Biometrická vlastnost	Index komfortu	Index přesnost	Index dostupnosti	Index ceny
Otisk prstů	7	7	4	3
Dynamika podpisu	3	4	5	4
Geometrie tváře	9	4	7	5
Vzorek duhovky	8	9	8	8
Sítnice oka	6	8	5	7
Geometrie ruky	6	5	6	5
Geometrie prstu	7	3	7	4
Struktura žil zápěstí	6	6	6	5
Tvar ucha	5	4	7	5
Hlas, akustická křivka	4	3	3	2
DNA	1	7	9	9
Pach, struktura	?	2	7	?
Dynamika psaní na klávesnici	4	1	2	1
Srovnání: heslo	5	2	8	1

SROVNÁNÍ BIOMETRICKÝCH METOD

- V poměru cena a přesnost vychází nejlépe otisk prstu.
- Duhovka oka má vysoké hodnocení v případě, že cena nehraje roli.
- DNA ztrácí v komfortu snímání, je zdlouhavá (jednovaječná dvojčata jí mají shodnou).

STÁLOST BIOMETRICKÉ VLASTNOSTI V ČASE



- růst živé tkáně, opotřebení, biologické stárnutí, nečistoty, zranění, následným hojícím procesem, další nespecifikované vlivy.

MĚŘENÍ VÝKONNOSTI BIOMETRICKÝCH SYSTÉMŮ

Efektivnost biometrických systémů lze měřit statistickými koeficienty. Charakteristickými výkonnostními mírami jsou :

- Koeficient nesprávného přijetí, False Acceptance Rate (FAR).
- Koeficient nesprávného odmítnutí, False Rejection Rate (FRR).

- Chyby FRR a FAR jsou vyjádřeny v procentech, nebo poměrem. Např. FAR 0,001% odpovídá poměru 1: 100 000. V tomto případě to znamená, že jeden ze sto tisíc neoprávněných pokusů může být připuštěn do systému.

MĚŘENÍ VÝKONNOSTI BIOMETRICKÝCH SYSTÉMŮ

- Koeficient nesprávného přijetí, False Acceptance Rate (FAR) – udává index míry bezpečnosti toho, že **neoprávněná osoba je přijata jako oprávněná**. Označuje se jako chyba II. druhu. Jde o **přijetí neregistrované osoby do systému**. Jedná se o chybu velmi závažnou; kritickou z bezpečnostního i marketingové hlediska.

$$FAR = (N_{FA}/N_{IIA}) \times 100\ [\%]$$

N_{FA} - počet chybných přijeti
N_{IIA} – počet pokusů neoprávněných osob o identifikaci

- V komerční sféře ochraňující jakýkoliv osobní majetek je FAR nežádoucí. Pokud se na tuto problematiku podíváme z pohledu kriminalistiky, tak FAR vyjadřuje míru odsouzení nesprávných osob. FAR se zaměřuje na bezpečnost systémů, čím menší FAR, tím je systém bezpečnější.

MĚŘENÍ VÝKONNOSTI BIOMETRICKÝCH SYSTÉMŮ

- Koeficient nesprávného odmítnutí, False Rejection Rate (FRR) – udává index míry toho, že **oprávněný uživatel je systémem odmítnut**. Označuje se jako chyba I. druhu. **Z bezpečnostního hlediska nemá velký význam**. Jde o marketingově nevýhodnou chybu, nutí uživatele k opakování pokusu a jeho nespokojenost.

$$FRR = (N_{FR}/N_{EIA}) \times 100\ [\%]$$

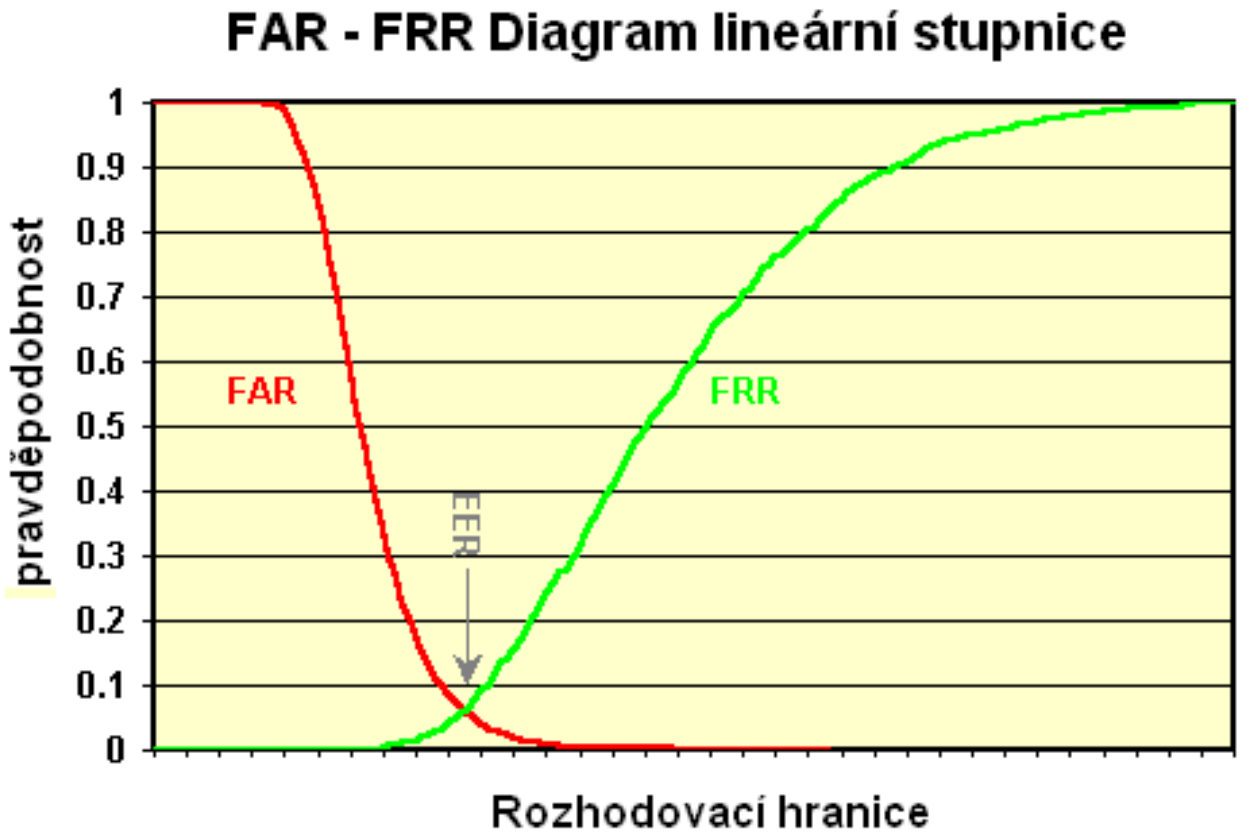
N_{FA} - počet chybných přijetí
N_{IIA} – počet pokusů neoprávněných osob o identifikaci

- Pokud bude mít nějaký biometrický prvek FRR vysoké, stává se nepoužitelným pro komerční účely, jelikož spousta uživatelů požaduje pohodlnost a tato skutečnost by je spíše frustrovala. Pokud se naopak podíváme na systémy používané v kriminalistice mají FRR vyšší. Potřebují, aby jejich systém byl naprosto bezchybný a nedocházelo k situacím, kdy systém není schopen identifikovat pachatele.

FAR / FRR

- Koeficient vyrovnané chyby, Equal error rate (EER) – Křížový koeficient je důležitým ukazatelem při nastavování citlivosti systému, udává ideální rozložení chyb FAR a FRR.

Biometrická charakteristika	FAR	FRR	Doba sejmutí a ověření
Otisk prstů	0,000 1 – 0,000 01 %	< 1,0 %	0,2 – 1 s
Geometrie ruky	0.1 %	0,1 %	1 – 2 s
Geometrie tváře	0,1 %	< 1,0 %	3 s
Obraz sítnice	0,001 %	0,4 %	1,5 – 4 s
Obraz duvovky	0.000 78 %	0,000 66 %	2 s
Charakteristika hlasu	Neuvádí se	Neuvádí se	1,5 s


FAR - FRR Diagram lineární stupnice
pravděpodobnost
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
FAR
FRR
EER
Rozhodovací hranice

FAR / FRR


RFID V BEZPEČNOSTNÍ
PRAXI

RFID

- RFID - *Radio Frequency Identification* – **radiofrekvenční identifikace**, tedy identifikace pomocí elektromagnetických vln
- digitální data zapsaná v RFID tagu, nebo „chytré etiketě“ přečtena snímačem za použití radiového elektromagnetického vlnění.
- navazuje na technologii čárových kódů, ale k zachycení dat z tagu používá radiové vlny (**bez přímé viditelnosti**) namísto optického snímání čárového kódu z etikety.
- automatická identifikace a sběr dat – umí **automaticky identifikovat objekty**, shromažďovat o nich data a zadávat tato data přímo do výpočetních systémů s minimálním nebo dokonce žádným zásahem člověka.
- drtivá většina přístupových a docházkových systémů využívá standardy LF (125kHz) a HF 13.56MHz).

DRUHY RFID FREKVENCÍ

Nízkofrekvenční (Low Frequency) 125 - 134 kHz

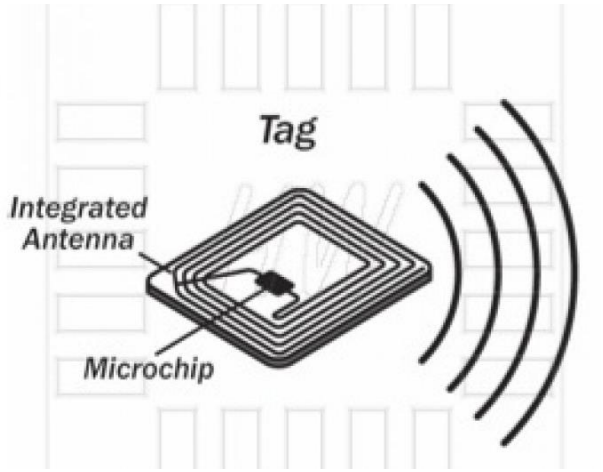
- Nízká frekvence, používá se hlavně pro sledování a označování zvířat, identifikaci osob, autorizaci - povolení přístupu v identifikačních kartách, klíčenkách. Čtecí rozsah je přibližně do 10 cm.

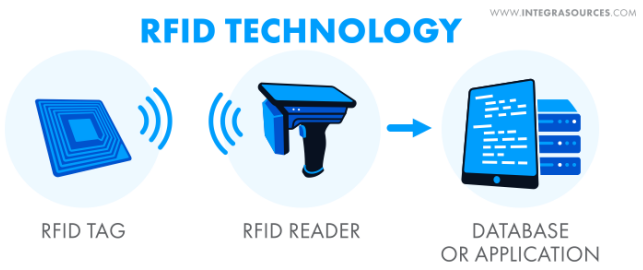
Vysokofrekvenční (High Frequency) 13,56 MHz

- Vysokofrekvenční systémy mají čtecí rozsah od 1 cm do 1 m. Součástí této frekvence je komunikace na krátkou vzdálenost - Near Field Communication (NFC). Tento rozsah se běžně používá pro platby, aplikace vstupenek, bezkontaktní karty, knihovní systémy a docházkové systémy, identifikační karty.

Ultra-vysokofrekvenční (Ultra-High Frequency - UHF) 865 - 960 MHz

- Nejvyužívanější frekvence u většiny RFID aplikací. V Evropě se používá EU norma a v souladu s tím zařízení fungují v pásmu 865 - 868 MHz. Čtecí rozsah pro pasivní UHF tagy je od několika centimetrů u malých tagů. U velkých tagů je to až do 10m. Tato frekvence se používá při sledování aplikací, zboží, řízení dodavatelského řetězce, ve výrobě, logistice a maloobchodě.





PRINCIP KOMUNIKACE

- RFID tag obsahuje integrované obvody a anténu, pomocí níž se přenáší data do RFID snímače.
- Informace jsou odesílány a načítány z RFID tagů pomocí snímače využívajícího radiové vlny.
- Snímač konvertuje elektromagnetické vlnění na digitální data
- Informace získané z tagů jsou následně snímačem odesílány přes komunikační rozhraní do hostitelského systému, kde mohou být data uložena v databázi a později analyzována.

PASIVNÍ / AKTIVNÍ ČIPY

- Pasivní systémy – nemá bateriíí, RFID snímač vytvoří elektromagnetické pole, které „vybudí“ tag a poskytne mu dostatek energie k napájení a pro odpověď prostřednictvím tzv. backscatteru. U pasivních čipů dochází k vysílání pouze v případě aktivace čtečkou. Jsou levnější a mnohem rozšířenější.
- Aktivní systémy – baterie umístěná v tagu zajišťuje zvýšení efektivního dosahu tagu a podporu dalších funkcí, které pasivní tagy nemají, například snímání fyzikálních veličin jako je teplota, tlak, vlhkost a pod. U aktivních transpondérů (pracují v pásmu 2,4 GHz), zde dochází k nepřetržitému vysílání datové informace. Jsou nákladnější.

RFID tag, co by nositel informace, může být ve formě etikety (Smart label) nebo v zapouzdřené podobě různých tvarů, velikostí a materiálů. Ke čtení a zapisování dat do RFID tagu slouží RFID čtečka, která může mít různou podobu (mobilní terminál, stacionární brána).

VLASTNOSTI RFID TECHNOLOGIE

- Není nutná přímá viditelnost mezi čtečkou RFID a tagem (štítkem)
- Tagy lze použít opakovaně
- Data uložená ve štítku (tagu) jsou šifrována a navíc mohou být chráněna heslem
- RFID tagy mohou obsahovat tištěné informace, jako jsou čárové kódy, názvy společností nebo jakýkoliv alfanumerický řetězec
- Mnohačetné snímání v krátkém čase
- Hromadné snímání v okolí čtecího zařízení
- Možnost vysoké rychlosti průjezdu identifikovaného objektu
- Odolnost vůči teplotě, vlhkosti a vlivům okolního prostředí (vysoká spolehlivost i za extrémních podmínek)
- Možnost aktualizace uložených informací a relativně velká kapacita dat
- RFID systémy lze integrovat do jiných interních systémů nebo zákaznických procesů

VYUŽITÍ V PRAXI

- správa zásob
- sledování majetku
- sledování osob
- řízení přístupu do vyhrazených prostor
- identifikace
- správa dodavatelských řetězců
- prevence padělání (například ve farmaceutickém průmyslu)

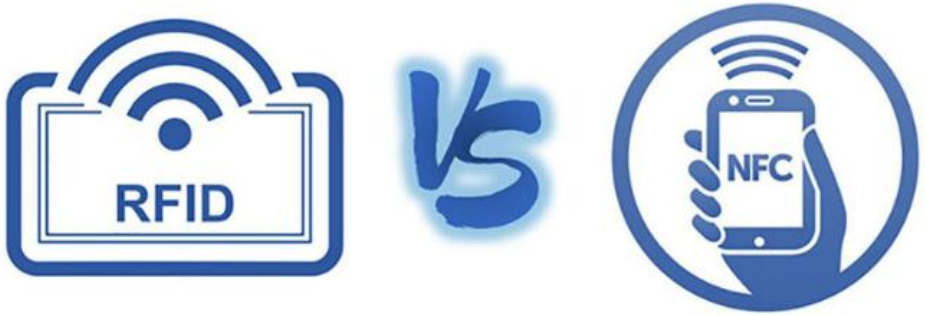
ZNEUŽITÍ ?

- Na většinu pasivních tagů s podporou EPC standardů se dá zapisovat pouze jednou (dostatečná ochrana)
- Tagy, podporující například standardy ISO, dovolují několikanásobné přepisování. Může být poměrně snadno modifikován hackery. RFID EPC 2. generace na pásmu UHF podporují dokonce několik tisíc přepsání.
- Povedlo se demonstrativně v roce 2004 na konferenci Black Hat. Byl použit malý program pro čtení a změnu údajů vdaném tagu (postačí správná čtečka propojená k PDA či notebooku s operačním systémem Windows či Linux.)
- Např. obchodní řetězec Tesco obdržel cenu Big Brother Awards a byl označen za největšího komerčního slídila proto, že tajně přidával RFID čipy do zboží a následně pak sledoval pohyb zákazníka.
- Teoreticky čtení citlivých údajů z biometrických pasů obsahujících RFID při vzájemném průchodu osob.

ZNEUŽITÍ A OCHRANA

- Pokud je peněženka, kapsa kabelky nebo aktovky (pouzdro na doklady atd.) opatřena RFID ochranou, tak je zpravidla lemována speciálními ochrannými RFID vlákny, které dokáží zablokovat příchozí bezdrátové komunikace a zamezí tak nežádoucímu čtení choulostivých dat z Vašich kreditních a bankovních karet.
- U kreditních, platebních či jiných typů BEZKONTAKTNÍCH karet je komunikace založena na RFID. Pokud se v blízkosti objeví pasivní RFID čip, využije přijímanou energii k nabití svého napájecího kondenzátoru a odešle odpověď zpět k vysílači. Tento způsob komunikace technicky umožňuje bez Vašeho vědomí zjišťovat osobní informace z Vaší karty.
- Máte-li svoji kartu nechráněnu dáváte ji všanc okolí s ní komunikovat. Proto je velmi vhodné efektivně zamezit komunikaci okolí s bezkontaktní kartou pomocí ochranného obalu.

(Zdroj: http://www.kartyvbezpeci.cz/content/9-bezpecnost-bezkontaktnich-platebnich-karet)



PODOBNÉ TECHNOLOGIE

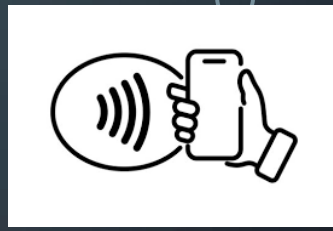
NFC

- NFC – Near Field Communication
- RFID je proces, kterým jsou prvky jednoznačně identifikovány pomocí rádiových vln, a NFC je specializovaná oblast v rámci rodiny technologie RFID. Konkrétně NFC je větev vysokofrekvenčního (HF) RFID a obě pracují na 13,56 MHz
- Technologie radiové bezdrátové komunikace mezi elektronickými zařízeními na velmi krátkou vzdálenost (do 4 cm). Tuto vzdálenost je však možno za použití většího výkonu a antény značně prodloužit.
- NFC je bezdrátová technologie umožňující rychlou a zabezpečenou výměnu dat na vzdálenost do 4 cm. Podporuje ji řada chytrých telefonů a tabletů, přičemž díky velmi krátké vzdálenosti je bezpečná a není vyžadována jejich identifikace.

NFC

- NFC čipy pracují na stejné frekvenci (13,56 MHz) jako HF RFID čtečky a štítky
- Jako vylepšená verze HF RFID využila zařízení pro komunikaci v blízkém poli výhody krátkého čtecího dosahu kvůli omezení své rádiové frekvence. Vzhledem k tomu, že zařízení NFC musí být blízko sebe, obvykle ne více než několik palců, staly se oblíbenou volbou pro zabezpečenou komunikaci mezi spotřebitelskými zařízeními, jako jsou např. smartphony, dveře atd.
- Peer-to-peer komunikace je funkce, která odlišuje NFC od jednoho z typických RFID zařízení. Zařízení NFC může fungovat jako čtečka i jako štítek. Tato jedinečná schopnost učinila z NFC oblíbenou volbu např. bezkontaktní platby.
- Níže jsou uvedeny některé normy ISO a typy čipů používané v souvislosti s plastovými kartami a přívěsky na klíče: ISO 15693, 18003, 14443A, 14444B, 18000

VLASTNOSTI NFC TECHNOLOGIE



- Rozhraní NFC je již integrováno do téměř všech mobilních telefonů
- NFC je celosvětově standardizováno a lze jej použít v rozsáhlém měřítku – průmysl, logistika, marketing, sektor automotive atd.
- Není zapotřebí speciální aplikace
- Tato standardizovaná mezinárodní digitální platforma se nachází na frekvenci 13,56 MHz a je založena na normě ISO14443 resp. ISO15693
- Odstup do vzdálenosti max. 5 cm a rychlé vytvoření spojení
- Každý NFC disponuje celosvětově jedinečným identifikačním číslem (zpětné sledování)
- Neviditelná integrace do současného designu, neboť není zapotřebí vizuálního kontaktu se smartphonem.
- Téměř 100% podíl správného načtení při prvním pokusu
- Údaje na čipu lze kdykoliv doplnit, načíst a změnit

NFC – POUŽITÍ V PRAXI

Platební systémy:

- Postupný přechod platebních systémů (tzv. Smartcards) a terminálů.

Integrace do chytrých telefonů:

- Nejčastěji se ve spojení se službami Google Pay (Android) nebo Apple Pay (iOS) využívá jako náhrada fyzické platební karty. Integrace do hodinek.

Propojení zařízení (pairing) a přenos dat:

- velice rychlé párování zařízení mezi sebou, např. propojení telefonů mezi sebou (sdílení kontaktů, fotografií, videí, …), připojení různých periferií (koncové prcky k ústředně, párování sluchátek k telefonu aj.) Přenos dat dále probíhá prostřednictvím Bluetooth

Identifikace:

- NFC Forum má zájem o to, aby se NFC využívalo pro identifikaci osob a zařízení (náhrada elektronické identifikační karty a klíčenky s čipem), prokazování totožnosti osob apod.

Emulace přístupových karet:

- Chytrý telefon přebírá funkci vstupní karty (otevírání dveří hotelového pokoje, přístup do společnosti včetně logu doby přístupu).

NFC VS RFID

NFC vs RFID:

https://www.youtube.com/watch?v=m0wXeSxQj9I

https://www.youtube.com/watch?v=5P0ws85j9zU&t=3s

DARK SIDE – BEZPEČNOSTNÍ HROZBA

Jsi v bezpečí před Flipper Zero? Co všechno lze “ukrást” pomocí hračky za pár tisíc?

https://www.youtube.com/watch?v=LSjCmx5T9w8&t=1s