

Biometrické systémy EKV

Doc. Ing. Karel Burda, CSc.



Program

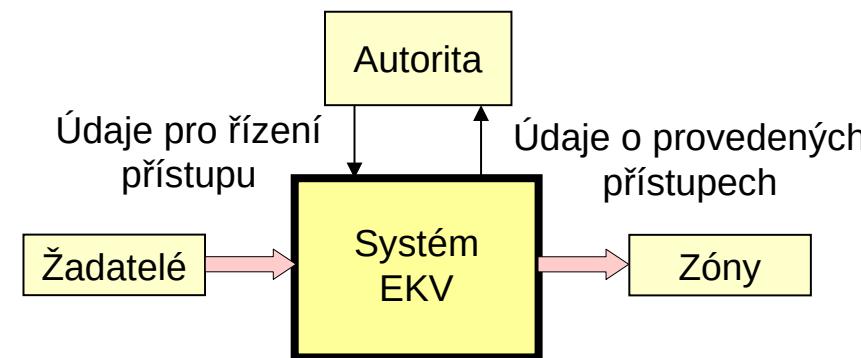
Biometrické systémy EKV

1. Úvod
2. Biometrické systémy EKV
3. Typy biometrických autentizací
4. Vlastnosti biometrických autentizací
5. Elektronické a mechanické zabezpečení
6. Závěr

1. Úvod

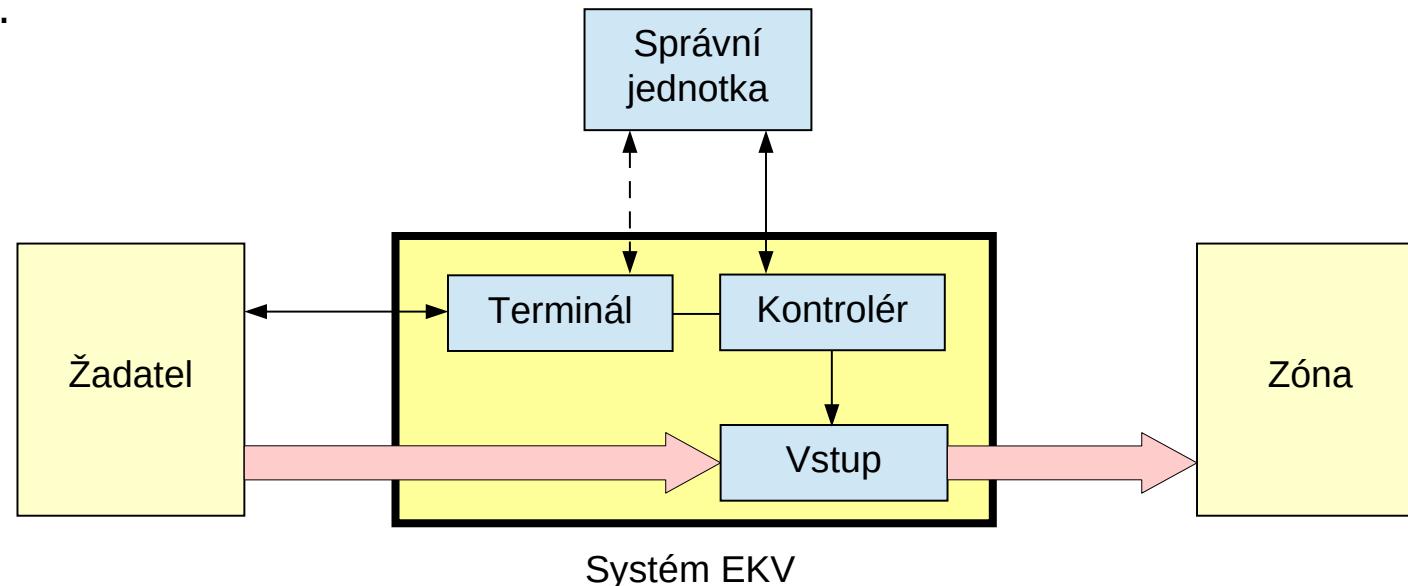
Základní pojmy

- **Biometrika**: číselně vyjádřená **morfologická**, nebo **behaviorální** charakteristika osoby (např. obrazec papilárních linií prstu nebo způsob chůze).
Pozn.: **Morfologické** = týkající se vzhledu,
Behaviorální = týkající se chování.
- **Systém EKV**: elektronický systém určený k automatizovanému řízení vstupů kontrolované oblasti
- **Biometrické systémy EKV**: systémy EKV, v nichž jsou osoby autentizovány pomocí jejich biometrik.
- **Zóna**: oblast ohrazená překážkami, do níž mohou vstupovat pouze autorizované osoby.
- **Žadatel**: osoba žádající o přístup do zóny.
- **Autorita**: osoba, který rozhoduje o tom, kdo a podle jakého časového rozvrhu smí do zón vstupovat (tj. jaká má práva).



Architektura systému EKV

- **Kontrolér**: řídící jednotka systému EKV.
- **Vstup**: uzavíratelný průchod, který je elektricky ovládán kontrolérem. Obvykle se jedná o dveře s elektrickým zámkem.
- **Terminál**: zařízení pro komunikaci osoby se systémem EKV. Obvykle se jedná o čtečku biometriky (např. otisku prstu), čtečku karet, klávesnici pro vložení hesla nebo případně nějakou kombinaci uvedených zařízení.
- **Správní jednotka**: zařízení pro správu systému EKV. Obvykle se jedná o počítač se specializovaným softwarem. U systémů s biometrickou a mikropočítákovou autentizací správní jednotka obvykle komunikuje i s terminálem (kvůli správě ověřovacího seznamu).



2. Biometrické systémy EKV

Biometrická autentizace

- Biometrická autentizace (alias autentizace žadatelem) je autentizace, v níž je dokazovacím faktorem DF biometrika žadatele.
- Vzhledem k výpočetním a přenosovým nárokům se biometrická autentizace neprovádí v kontroléru, ale provádí se v terminálu.
- Autorita v rámci autorizace nejprve změří žadatelovu biometriku. Záznam této biometriky tvoří soubor, který se nazývá šablona.
- Šablona je ověřovacím faktorem OF, který se ukládá v terminálech. Případně může být šablona digitálně podepsána autoritou a žadatelé si ji nosí ve svém hardware (např. v mikropočítačové kartě). V takovémto případě terminál šablonu nevyhledává ve své paměti, ale načte si ji z karty žadatele.
- Při žádosti o přístup žadatele dostane terminál od svého biometrického snímače aktuálně změřenou biometriku žadatele (tzv. dokazovací data DD) a porovnává ji se šablonou (OF). Podle míry shody DD a OF rozhoduje terminál o úspěšnosti autentizace.
- Pokud je autentizace úspěšná, tak terminál zašle kontroléru ID žadatele (obvykle Wiegandovo slovo). Kontrolér podle přístupového seznamu zjistí práva žadatele a podle toho ovládá vstup.

Autentizace rozpoznáváním a oznamením

- Pokud je **šablona** uložena **v terminálu**, tak se používá **rozpoznávací autentizace**. Terminál v autentizačním testu postupně pro zjištěná DD **zkouší** jednotlivé OF. Pokud zjistí dostatečnou podobu DD a OF osoby s ID_X, tak je žadatel považován za osobu **X**. Zjištěný identifikátor ID je zaslán kontroléru.
- Soudobé terminály mají kapacitu N řádově **tisíce šablon** a všechny tyto šablony dokáží pro sejmutou biometriku žadatele (tj. DD) vyzkoušet **do 1 sekundy**.
- Pokud je **šablona** uložena **v hardware** žadatele (typicky biometrický pas), tak se používá **oznamovací autentizace**. V tomto případě musí být terminál navíc vybaven vhodným **rozhraním** pro komunikaci s tímto hardwarem (typicky se jedná o čtečku karet). Terminál vyčte podepsanou šablonu z hardware a **veřejným klíčem** autority (ten je trvale uložen v terminálu) ověří autentičnost šablony. Z šablony se dozví i ID žadatele. Žadatelova DD následně porovná s šablonou a v případě jejich dostatečné podoby odešle ID žadatele do kontroléru. V opačném případě je autentizace neúspěšná.
- Pokud je hardware pro uložení certifikátu a šablony dostatečně **výkonný**, tak jej lze použít současně k hardwarové autentizaci. Tím je možná **dvoufaktorová** autentizace (biometrikou i hardwarem).
- Rozpoznávací autentizace se někdy označuje jako tzv. ověření typu **1:N** či také zmatečně jako identifikace. Oznamovací autentizace se označuje i jako tzv. ověření typu **1:1**.

3. Typy biometrických autentizací

Typy biometrické autentizace

- Třídy biometrické autentizace:
 - a) **morfologická**: využívá se unikátní **vzhled** osob (tzv. morfologické charakteristiky).
 - b) **behaviorální**: využívá se unikátní **chování** osob (tzv. behaviorální charakteristiky).
- **V praxi** se často využívají biometriky:
 - a) **otisků** prstů,
 - b) **cévního** řečiště prstu nebo dlaně,
 - c) geometrie **ruký**,
 - d) geometrie **obličeje**,
 - e) skvrn oční **duhovky**,
 - f) cévního řečiště oční **sítnice**,
 - g) **hlasu**,
 - h) způsobu **psaného** podpisu,
 - i) způsobu psaní na **klávesnici**.
- V systémech **EKV** se používají **výhradně morfologické** techniky autentizace. Důvodem je skutečnost, že sejmutí způsobu chování je časově náročnější než sejmutí morfologických charakteristik. Morfologické techniky autentizace tak umožňují **vyšší propustnost vstupů**.

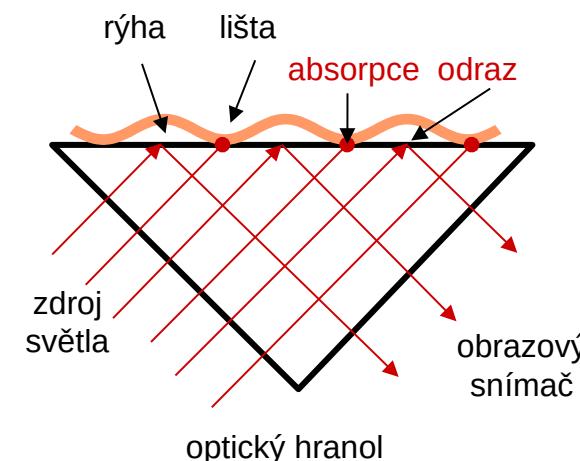
Autentizace podle otisků prstů

- **Papilární linie** jsou souvislé, líniové reliéfy na povrchu bříšek prstů. Tyto reliéfy jsou dány (viz obr. vlevo) střídáním vyvýšených linií (tzv. **lišt**) a snížených linií (tzv. **rýh**). Na otisku papilárních linií (viz obr. vpravo) mají lišty tmavou barvu a rýhy jsou světlé.
- Autentizace otiskem prstu je založena na faktu, že pravděpodobnost shody obrazce papilárních linií dvou osob je cca $64 \cdot 10^{-9}$. Obrazce papilárních linií jsou tak unikátní (viz například využití v daktyloskopii) a zároveň je lze snadno snímat.
- K pořízení obrazce papilárních linií se používají následující čtečky:
 - **obrazové čtečky**: obrazec papilárních linií se snímá obrazovým snímačem,
 - **kapacitní čtečky**: obrazec papilárních linií se snímá kapacitním snímačem,
 - **ultrazvukové čtečky**: obrazec papilárních linií se snímá sonarovým snímačem.



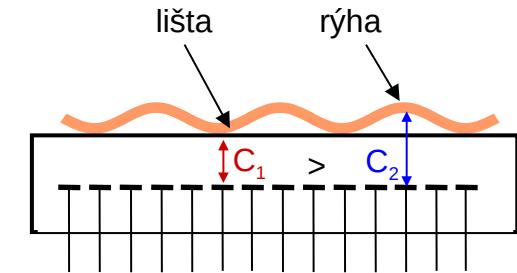
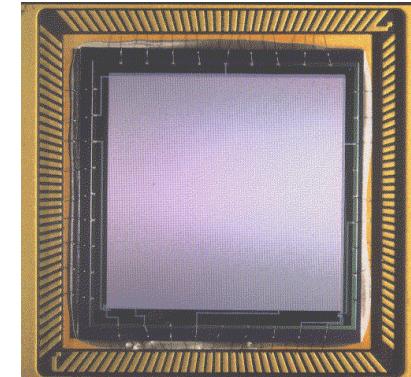
Obrazová čtečka otisku prstu

- U obrazové čtečky (obr. vlevo) se papilární linie snímají **obrazovým snímačem**.
- Obvykle osoba přiloží prst na stěnu optického **hranolu**, který je ozařován **světelným zdrojem** (obr. uprostřed). Fotony světla, které dopadnou na odražnou stěnu hranolu v místě, kde se nachází rýha (tj. na rozhraní sklo-vzduch) jsou odraženy směrem k obrazovému snímači. Fotony dopadající v místech kontaktu kožní lišty a skla jsou pohlceny tkání prstu.
- Pomocí obrazového snímače (zpravidla **CCD** nebo **CMOS** snímač) se z odražených fotonů vytvoří fotografický snímek papilárních linií, který se následně analyzuje.
- Vlastnosti: nízká **cena** a odolnost vůči **elektrostatické elektřině**. Nutnost **čištění** snímací stěny hranolu a nemožnost pořídit kvalitní obraz papilárních linií pokud je prst **umazaný**.
- Nejmodernější snímače fotografují otisky **více** prstů máchnutím ruky v prostoru snímače, tj. snímají bez potřeby se dotýkat optického hranolu (obr. vpravo).



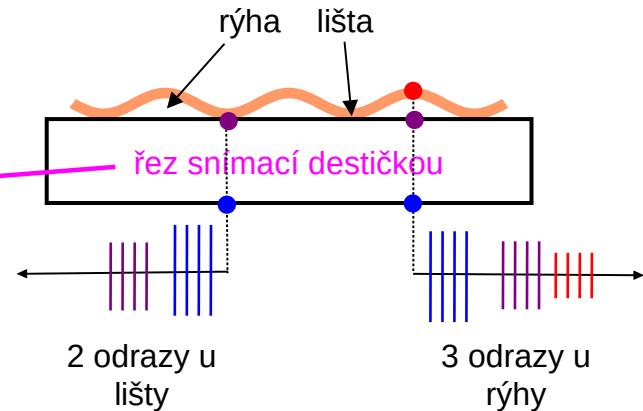
Kapacitní čtečka otisků prstů

- Kapacitní čtečky (obr. vlevo) zjišťují obraz papilárních linií měřením kapacity.
- Ke snímání se obvykle používá maticový snímač (obr. uprostřed) tvořený velkým počtem vodivých plošek, které jsou uspořádány do matice a zality v izolační destičce. Prst je kovovým rámečkem po obvodu snímače uzemněn. Poté se měří kapacita každé plošky snímače vůči prstu, tj. vůči zemi.
- Pokud se nad ploškou (obr. vpravo) nachází kožní lišta, tak jsou obě desky elementárního kondenzátoru (tj. ploška a kůže) vzdáleny jen o tloušťku dielektrické vrstvy. Je tak naměřena poměrně vysoká kapacita C_1 . Pokud se nad ploškou nachází rýha, tak vzdálenost mezi deskami elementárního kondenzátoru je o hloubku rýhy větší a kapacita C_2 je tak nižší.
- Z matice hodnot kapacit se vytvoří matice obrazových bodů obrazce papilárních linií.
- Vlastnosti: snímací plochu není zapotřebí čistit a snímače jsou schopny sejmout obrazec papilárních linií i v případě umazaného prstu. Jejich cena je přijatelná. Nevýhodou je možnost poškození elektrostatickým výbojem.



Ultrazvuková čtečka otisků prstů

- U ultrazvukové čtečky (obr. vlevo) se obrazec papilárních linií zjišťuje na principu **sonaru**.
- Pod snímací destičkou čtečky je matice piezoelektrických měničů, které fungují jako generátory i jako snímače. Generátor vygeneruje velmi krátký **pulz** akustické energie v **ultrazvukovém** pásmu. Na spodní části snímací destičky (na obr. vpravo modré body) se část akustického vlnění odrazí zpět (modré vlnoplochy) a snímač tak detekuje **první** odraz.
- Na horní ploše snímací destičky (fialové body) dojde ke **druhému** odrazu, který opět přijímač detekuje (fialové vlnoplochy).
- Pokud se ve snímaném bodě nachází lišta, tak je zbytek energie pulzu pochlben tkání. V případě **rýhy** se však vlnění šíří dále až ke kůži. Na tomto rozhraní (červený bod) se část energie vlnění odrazí a je přijímačem detekována jako **třetí** odraz (červené vlnoplochy).
- Vlastnosti: nevyžaduje **údržbu** a čištění. Je **odolný** vůči elektrostatické elektřině a dokáže snímat **umazané** prsty. Nevýhodou je vyšší **cena**.



Markanty

- Pomocí čteček z předchozích snímků jsme **získali obrazec** papilárních linií.
- V získaném obrázku se pak pomocí specializovaného software vyhledávají **specifické útvary** (např. konec lišty, rozvětvení lišty apod.), které se nazývají **markanty** (viz obrázek).
- Při **autorizaci** se pro každý markant do **šablony** (tj. do OF) zapisuje jeho **typ a souřadnice**. Stejně se postupuje při **autentizaci**, kdy se tytéž údaje zapisují do dokazovacích dat (DD).
- Údaje z šablony a dokazovacích dat se pak **porovnávají** statistickými metodami na podobnost. Pokud je podoba dostatečná, tak je autentizace úspěšná.

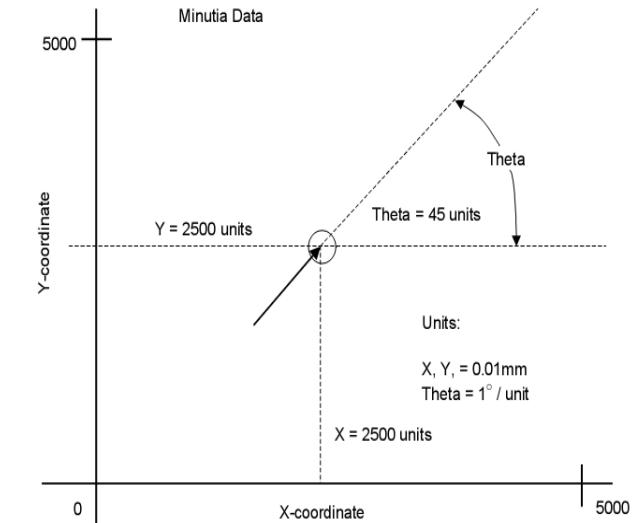
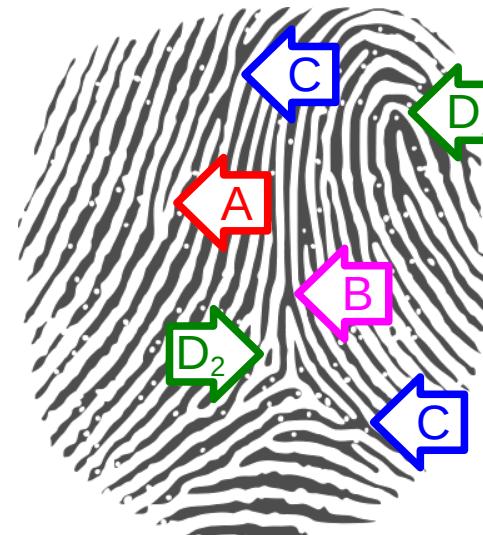


Popis otisků prstů

Typy v praxi sledovaných markantů:

- A: konec lišty,
- B: rozdvojení lišty,
- C: přechod, či roztrojení,
- D: jiné.

Např. D_1 je jádro a D_2 je ostrov.



Souřadnicový systém:

- X, Y: kartézské souřadnice markantu (rozsah 0 až 5 cm s krokem 0,01 mm = 10 μ m),
- Θ : úhel markantu (0 až 359 stupňů s krokem 1 stupeň),
 - u konce lišty (typ A): úhel, pod kterým lišta pokračuje (viz obrázek vpravo),
 - u rozdvojení lišty (typ B): úhel, pod kterým pokračuje vzniklá rýha,
 - u přechodu (typ C) a jiné (typ D): není definován.

Ochrana před útoky padělkem otisku prstu (1/3)

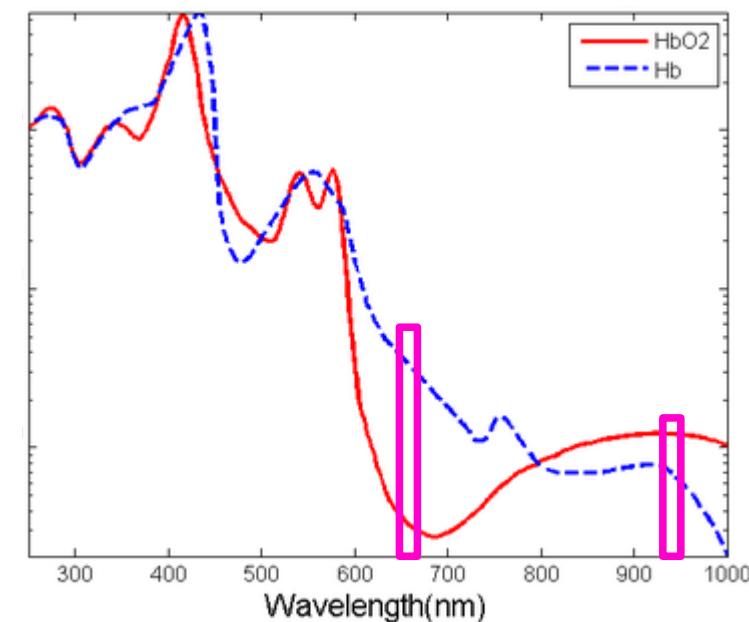
- Padělky obrazců papilárních linií se v praxi dělají ze **želatiny**, **silikonu** či různých **lepidel**.



- K detekci padělek otisků prstů se u optických snímačů zkoumá, zda je nosičem obrazce papilárních linií **tkání**. K tomu se nejčastěji využívají techniky založené na Rayleighově rozptylu.
- Rayleighův rozptyl** vzniká v důsledku ozařování látky, kdy fotony záření **interagují** s atomy ozařované látky (např. s atomy v lidské kůži).
- Ozařováním lidské kůže pomocí viditelného a infračerveného (IR) světla se srázejí fotony s elektrony atomů. Fotony **předají** elektronům svoji energii a tak **zaniknou**. Elektrony se dostanou na **vyšší** energetickou hladinu, avšak po určité době se **vrátí** na svoji základní energetickou hladinu. Dochází tím k vyzáření fotonu o stejně vlnové délce, jako měl excitační foton. Nově vzniklé fotony mají **náhodné** směry šíření a proto se nazývají Rayleighův **rozptyl**.

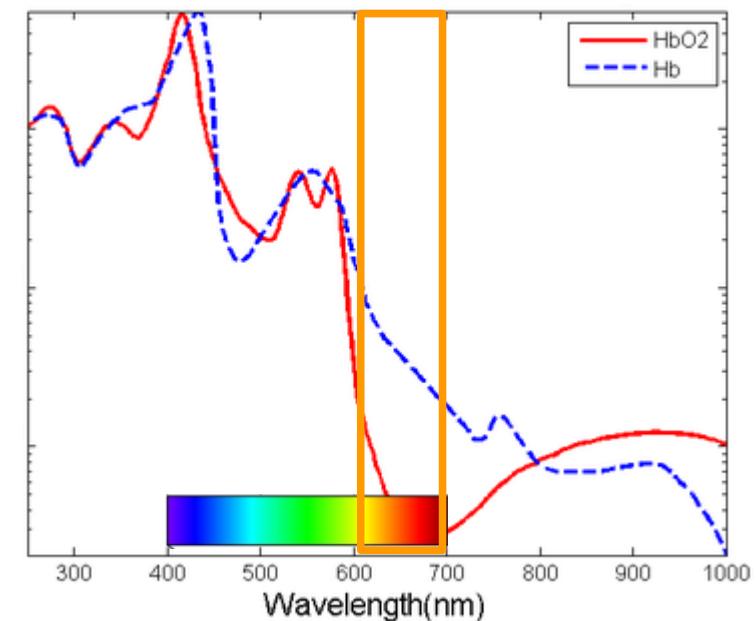
Ochrana před útoky padělkem otisku prstu (2/3)

- K ochraně před útokem modely otisků se používá:
 - čtečka s **pulzním oxymetrem**,
 - **multispektrální** čtečka.
- V obou případech se kontroluje **pulsování** krve v prstu.
- U varianty s pulzním oxymetrem se využívá skutečnost, že absorpcie Rayleighova záření krví v pásmu 660 nm a 940 nm (na obrázku označeny **fialově**) významně závisí na tom, zda je krev v prstu okysličena (**červený** průběh), či nikoliv (**modrý** průběh).
- V pásmu **660 nm** se intenzita Rayleighho záření **snižuje**, když **odkysličená** krev v žílách teče k srdci (absorpce u modrého průběhu je vyšší než u červeného průběhu). V pásmu **940 nm** je tomu **naopak**.
- Ozařováním, resp. prosvěcováním prstu v obou pásmech a porovnáním naměřených intenzit Rayleighova záření v čase jsme pak schopni detektovat krevní **pulz** v prstu, a tak se můžeme přesvědčit o tom, zda prst je **živý**.



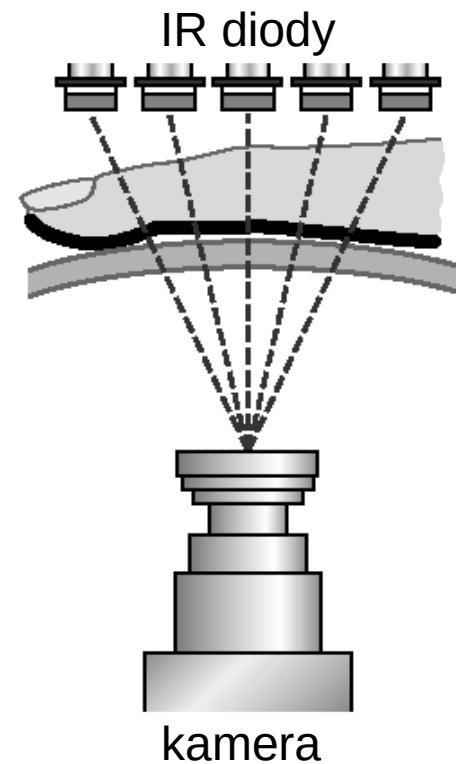
Ochrana před útoky padělkem otisku prstu (3/3)

- V případě **multispektrální** čtečky se prst ozařuje viditelným světlem s **různými** vlnovými délkami (obvykle modrým, zeleným, červeným a bílým světlem).
- Využívá se toho, že čím je vlnová délka větší, tím světlo pronikne do větší hloubky tkáně. Rayleighovo záření, které v dané hloubce vznikne se poté fotografuje, čímž získáme snímky papilárních linií z různých hloubek tkáně (obr. vlevo).
- Vzniklé fotografie se **integrují**, čímž spolehlivě získáváme kvalitní obraz papilárních linií i za nepříznivých okolností (suchý, mokrý nebo zamazaný prst).
- Dále se podobně jako u pulzního oxymetru využívá různá míra **absorpce červeného světla** (okolo 660 nm v oranžovém rámu na obrázku vpravo). Tím se opět měří pulz a tak se ověřuje, zda je snímaný prst živý.



Čtečka cévního řečiště prstu

- U čtečky cévního řečiště prstu (obr. vlevo) se prst **prosvěcuje** IR zářením (obr. uprostřed).
- Jak již víme, část IR fotonů je pohlcena hemoglobinem v krvi, takže cévy se pak na obrázku jeví **tmařší** (obr. vpravo).
- Oproti otiskům prstů mají autentizace cévním řečištěm výhodu, že obraz cévního řečiště osoby **není** běžně dostupný.

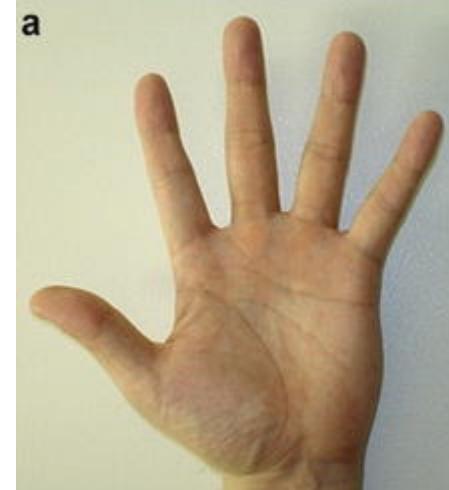


Čtečka cévního řečiště dlaně

- I u čtečky cévního řečiště dlaně (obr. vlevo) se využívá skutečnost, že **hemoglobin** pohlcuje fotony v IR pásmu 760 nm.
- Nasvícením dlaně IR zářením se v důsledku **Rayleighova** rozptylu objeví na snímku dlaně tmavé čáry, což jsou žíly. Digitálním zpracováním snímku se zvýší kontrast a vyextrahuje se úplná mapa cévního řečiště dlaně (viz obrázky a, b a c vpravo).
- Podobně lze autentizovat osoby také cévním řečištěm **hřbetu ruky**.

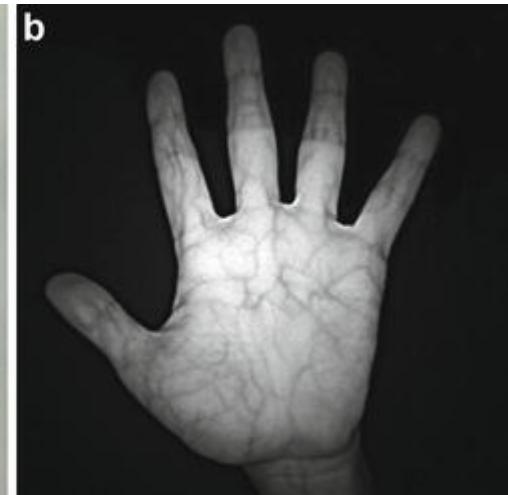


a



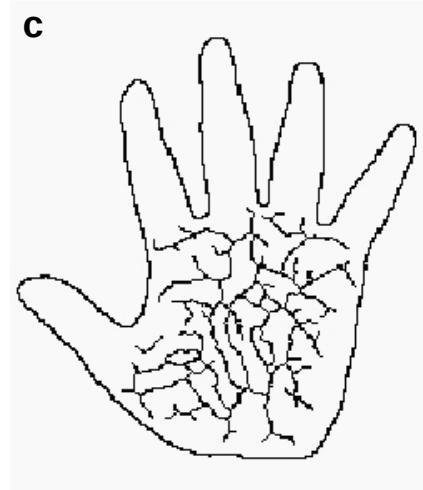
obrázek dlaně ve
viditelném spektru

b



obrázek dlaně v
IR spektru

c

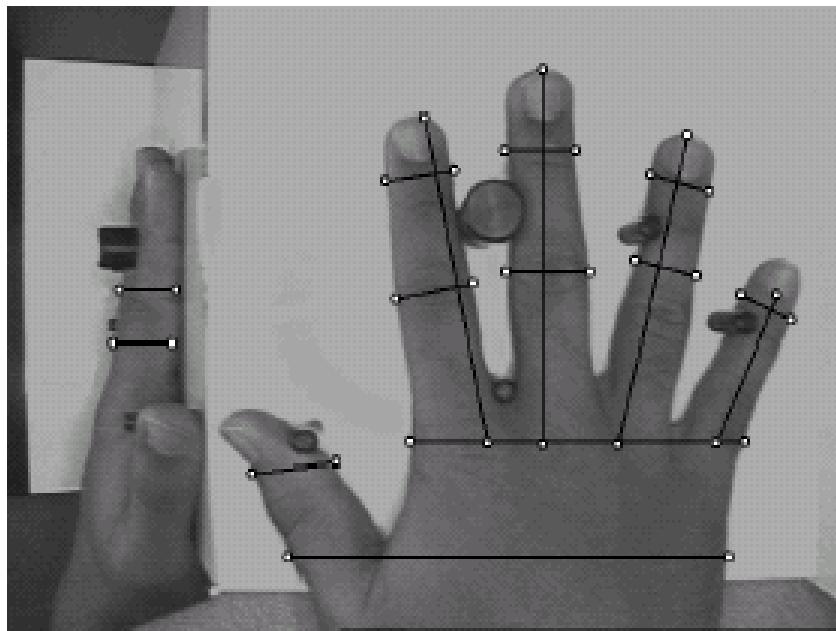


mapa cévního
řečiště

Autentizace podle geometrie ruky

Autentizace podle **geometrie ruky**:

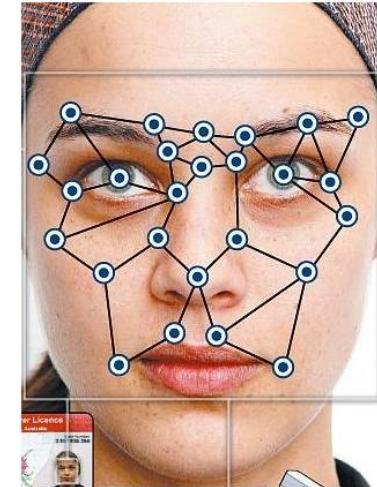
- Je založena na individuálních geometrických rozměrech lidské ruky. Ke snímání se používá optický snímač, kterým se získají fotografie ruky při pohledu shora a z boku.
- Z fotografií se získají základní **rozměry ruky** (např. délka a šířka prstů), získané údaje se zakódují a uloží.
- Uvedená metoda není příliš přesná, ale je poměrně laciná.



2D autentizace podle obličeje

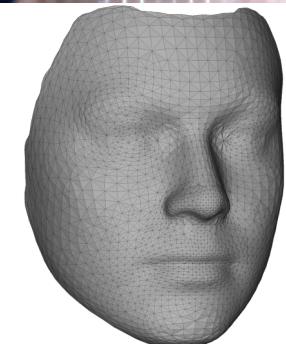
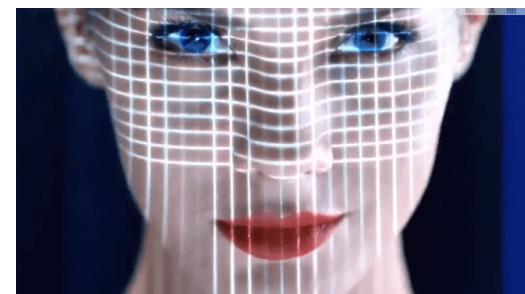
2D autentizace podle **obličeje**:

- Ke snímání postačí obyčejná kamera s dostatečným rozlišením. Autentizovaná osoba se nechá vyfotografovat zepředu a získaný portrét se dále zpracovává (obr. vlevo).
- Zpravidla se používá metoda **obličejobré metriky** (obr. uprostřed), kde se v obrázku naleznou významné body (např. koutky úst či očí, vrchol nosu apod.) a mezi těmito body se změří vzdálenosti.
- Autentizace podle obličeje je poměrně nespolehlivá a nepřesná metoda. Často lze autentizační zařízení **oklamat** fotografií nebo videem. Z tohoto důvodu jsou nyní nabízeny čtečky pro 3D autentizaci, které snímají obličeje jako **třírozměrný objekt** (oba obrázky vpravo).



3D autentizace podle obličeje

- U tohoto typu autentizace se využívá jev, kdy v důsledku různých **zakřivení** objektu se jím odražené fotony vracejí pod různými úhly, čímž dojde k deformaci obrazu objektu. Známým příkladem tohoto jevu jsou křivá zrcadla (obrázek nahoře) nebo obraz tváře na neklidné vodní hladině.
- V případě 3D autentizace podle obličeje se obličeji **nasvítí pravidelným rastrem**, který sestává řádově z desetitisíců bodů. K nasvícení se používá IR záření, takže autentizaci lze provádět i ve špatných světelných podmínkách.
- Z prostředního obrázku vidíme, že odražené paprsky vytvoří na fotografii obličeje rastr, jehož body už **nejsou** pravidelně vzdáleny. Na obrázku to je markantní na hřbetu nosu. Tyto nepravidelnosti se **vyhodnocují** a na jejich základě se vytvoří 3D model obličeje (obrázek dole).
- Ve 3D modelu obličeje se stejně jako u 2D modelu určí významné body, podle jejichž **vzájemné vzdálenosti** se provádí autentizace.



Autentizace duhovkou

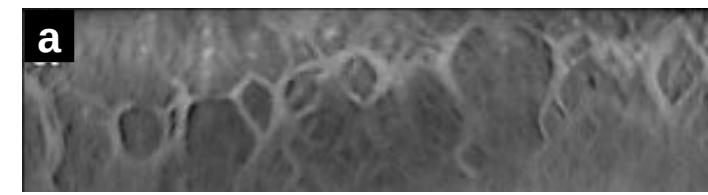
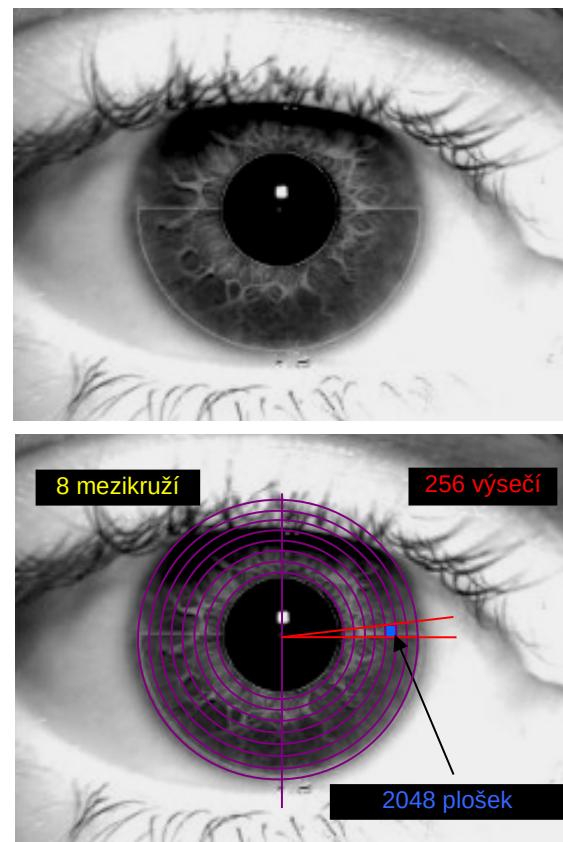
Autentizace podle **duhovky**:

- Metoda je založena na individuálnosti rozmístění a tvaru skvrn na duhovce lidského oka.
- Příklad spolehlivosti autentizace: Snímek dvanáctileté dívky z Afghánistánu a snímek téže osoby po 18 letech.

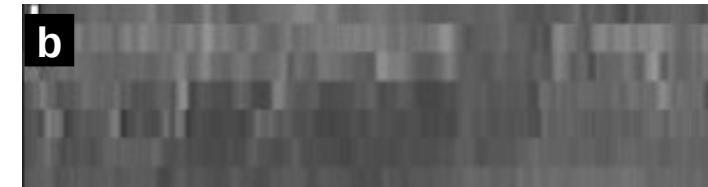


Princip autentizace duhovkou

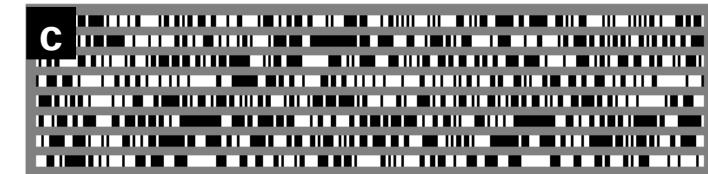
- Metoda je založena na **individuálnosti** rozmístění a tvaru **skvrn** na duhovce lidského oka. Ke snímání postačí obyčejná kamera s dostatečným rozlišením. Po vyfotografování očí osoby se ze získaného obrázku zjistí charakteristické znaky oční duhovky, které se kódují (**vlnková transformace**) a uloží do paměti. Metoda je velmi spolehlivá, avšak zatím patentově chráněná.



Obraz duhovky převedený do kartézských souřadnic.



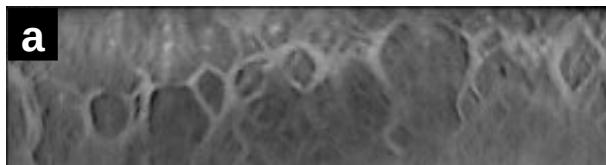
Obraz duhovky zprůměrovaný po ploškách.



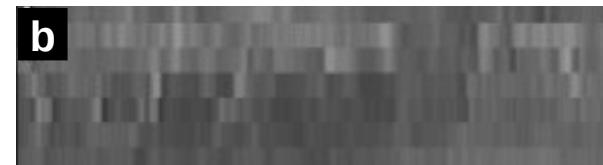
Výsledná biometrika duhovky (8x256 bit).

Postup při autentizaci duhovkou

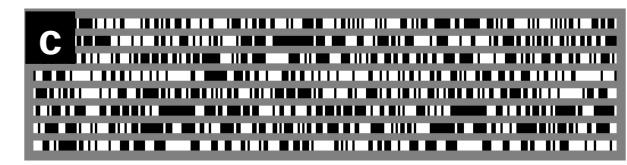
1. Duhovka se černobíle vyfotografuje a údaje o **barvě** pixelů se převedou z **polárních souřadnic** do **kartézských**. Obraz duhovky je tak převeden z podoby mezikruží do podoby obdélníku (obr. a).
2. Obdélník obrazu duhovky je rozdělen do **8 řádků** a **256 sloupců**, tj. do **2048 plošek**.
3. Hodnoty barev pixelů každé plošky jsou **zprůměrovány** (obr. b). Vznikne tak matice **A** o formátu 8×256 čísel, kde číslo a_{ij} reprezentuje **střední hodnotu barvy** pixelů plošky v i -tém řádku a j -tém sloupci.
4. Matice **A** se **vlnkovou** transformací převede na matici **B**. Každý prvek b_{ij} potom unikátním způsobem **závisí** na **všech** prvcích matice **A**.
5. Z matice **B** se odvodí matice **C** tak, že pokud $b_{ij} > 0$, tak $c_{ij} = 1$. Jinak $c_{ij} = 0$. Matici **C** potom můžeme reprezentovat jako **posloupnost** $8 \times 256 = 2048$ bitů (obr. c).
6. Při **autorizaci** $\mathbf{C} = \mathbf{OF}$ a při autentizaci $\mathbf{C} = \mathbf{DD}$. Pokud potom $\mathbf{OF} \approx \mathbf{DD}$, tak je autentizace **úspěšná**.



Obraz duhovky převedený do kartézských souřadnic.



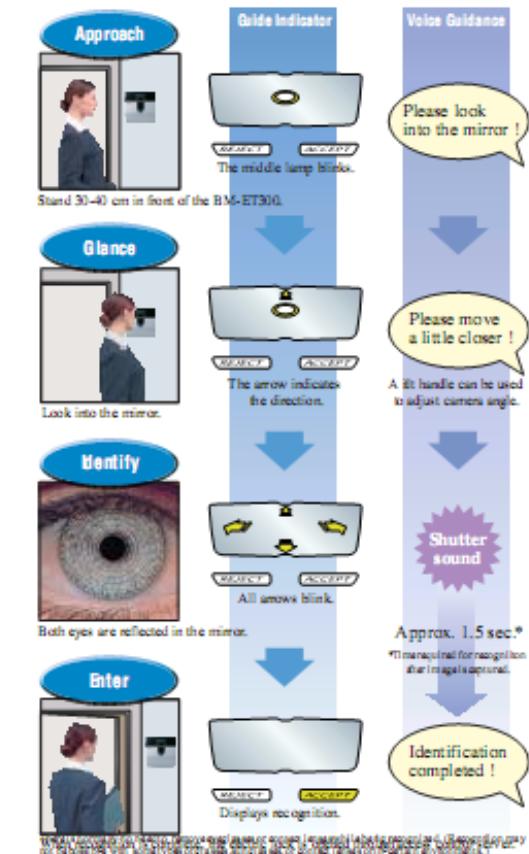
Obraz duhovky zprůměrovaný po ploškách.



Výsledná biometrika duhovky (8×256 bit).

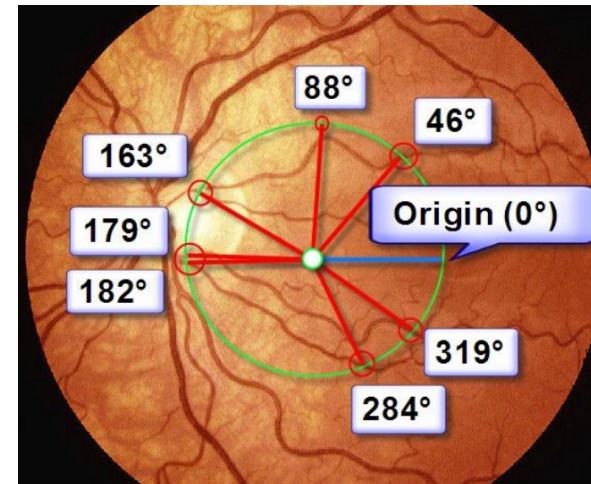
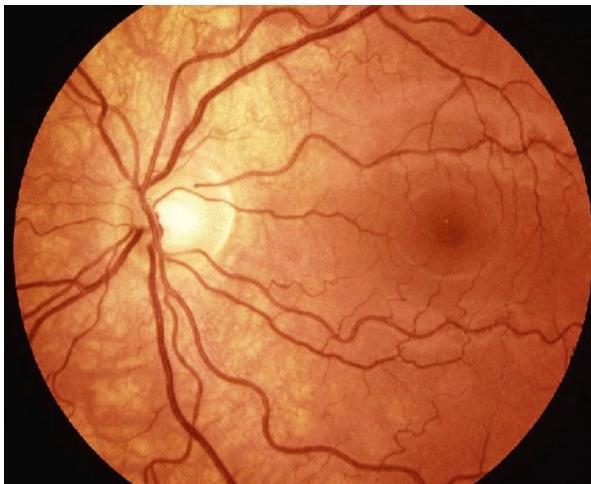
Autentizace duhovkou v praxi

- Zařízení pro autentizaci pomocí duhovky:



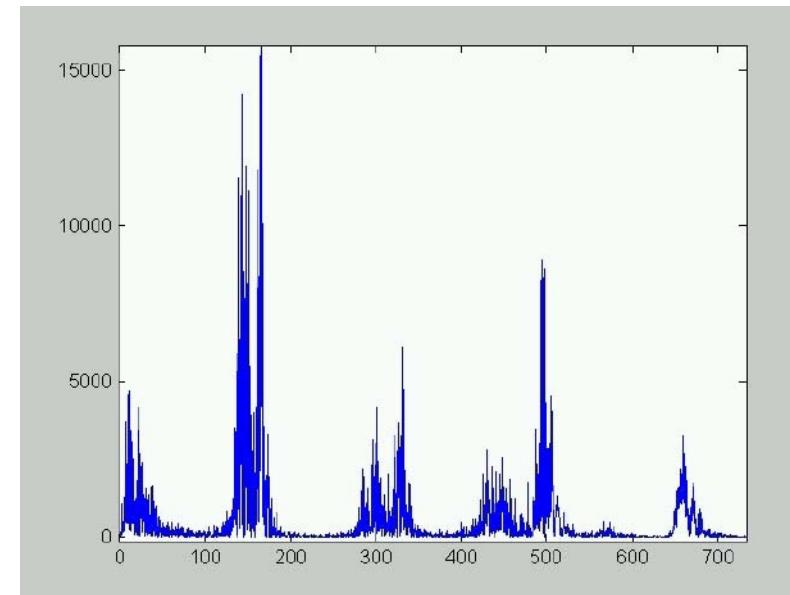
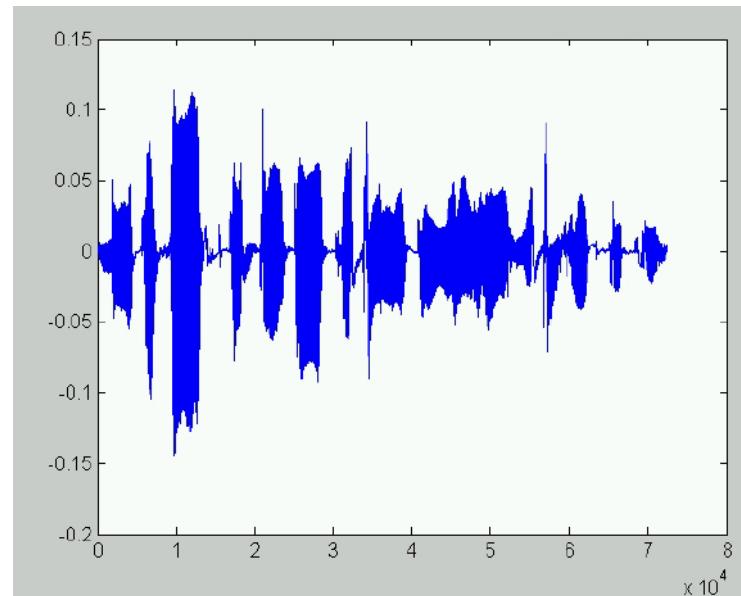
Autentizace podle oční sítnice

- Metoda je založena na individuálních rysech **cévního řečiště** oční **sítnice** (obr. vlevo).
- V autentizačním terminálu (obr. vpravo) je ke snímání zapotřebí speciální kamera s laserovým infračerveným paprskem.
- Laser ozáruje sítnici v kružnici (zelenou barvou). Cévy, které tuto kružnici protínají, se na snímku jeví jako **tmavé body** (obr. uprostřed). Rozmístění těchto bodů na kružnici je pro každou osobu unikátní.
- Osoba musí mít při autentizaci široce otevřenou zornici a nesmí mrknout. Autentizace je tak pro uživatele dosti **nepříjemná** procedura. Samotná metoda je poměrně přesná, avšak drahá.



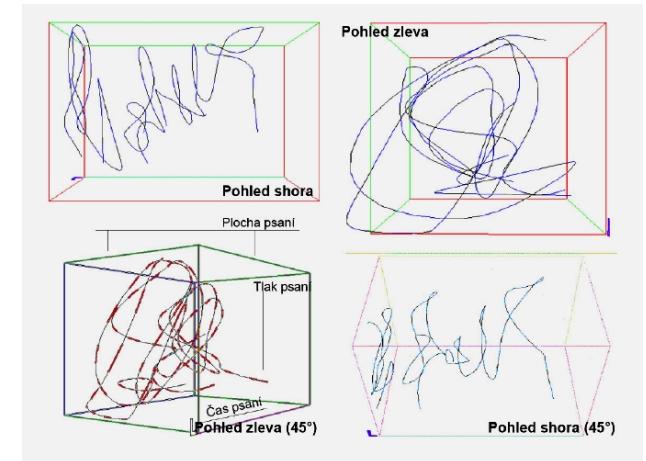
Autentizace hlasem

- **Behaviorální metody** se v biometrických přístupových systémech prakticky nepoužívají. Zmíníme je jen pro úplnost.
- Autentizace **podle hlasu** využívá specifické charakteristiky řečníka (např. kadenci řeči, kmitočtové spektrum hlasu apod.) při sdělení nějaké fráze. Ke snímání se využívají běžné mikrofony.



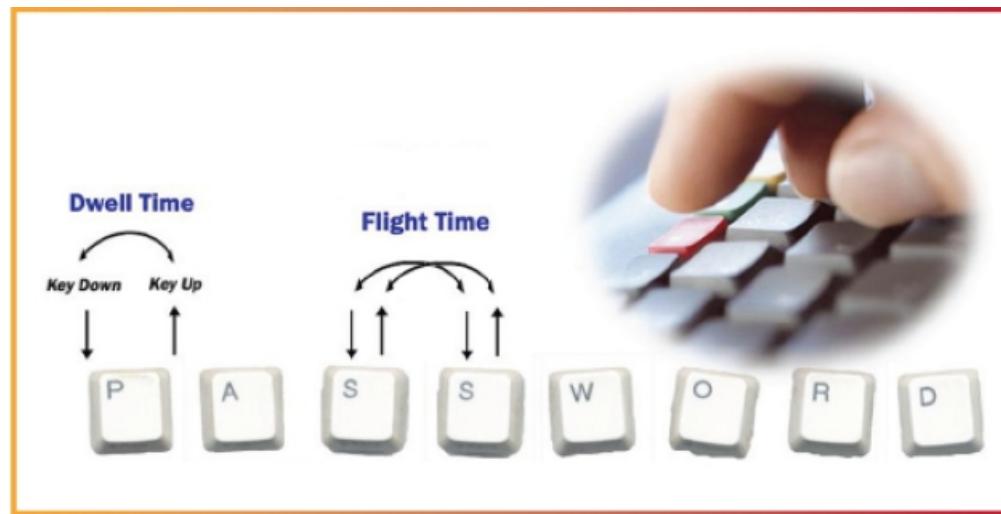
Autentizace způsobem podpisu

- Autentizace podle **způsobu podpisu** využívá individuálnost provedení ručního podpisu (dynamika, tlak na podložku, sklon pera apod.). Ke snímání postačují běžné dotykové snímače. Metoda není příliš přesná.



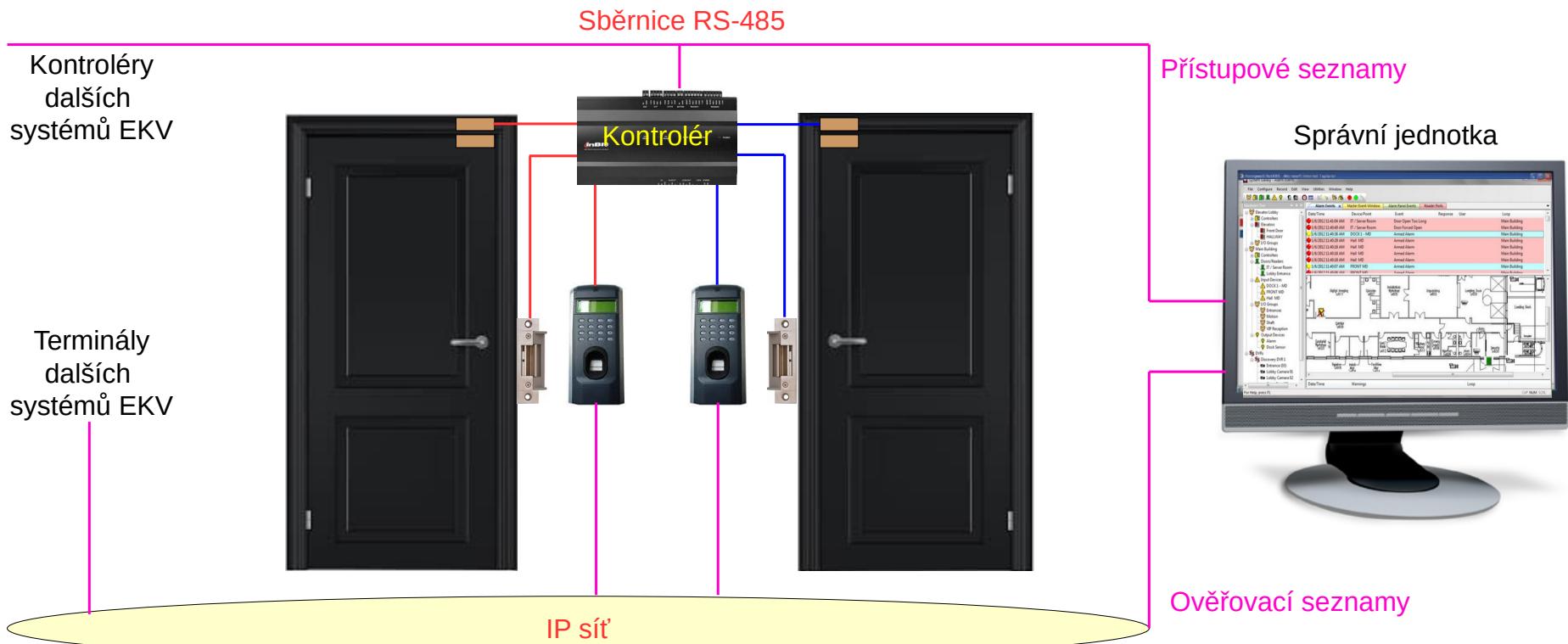
Autentizace psaním na klávesnici

- Autentizace podle **psaní na klávesnici** je založena na specifických rysech zápisu nějaké sekvence znaků (např. kadence psaní, délky pauz apod.). Ke snímání postačuje běžná klávesnice. Její výhodou je skutečnost, že autentizace nemusí být jednorázová, ale může být průběžná - po celou dobu práce v systému.



Správa biometrického systému EKV

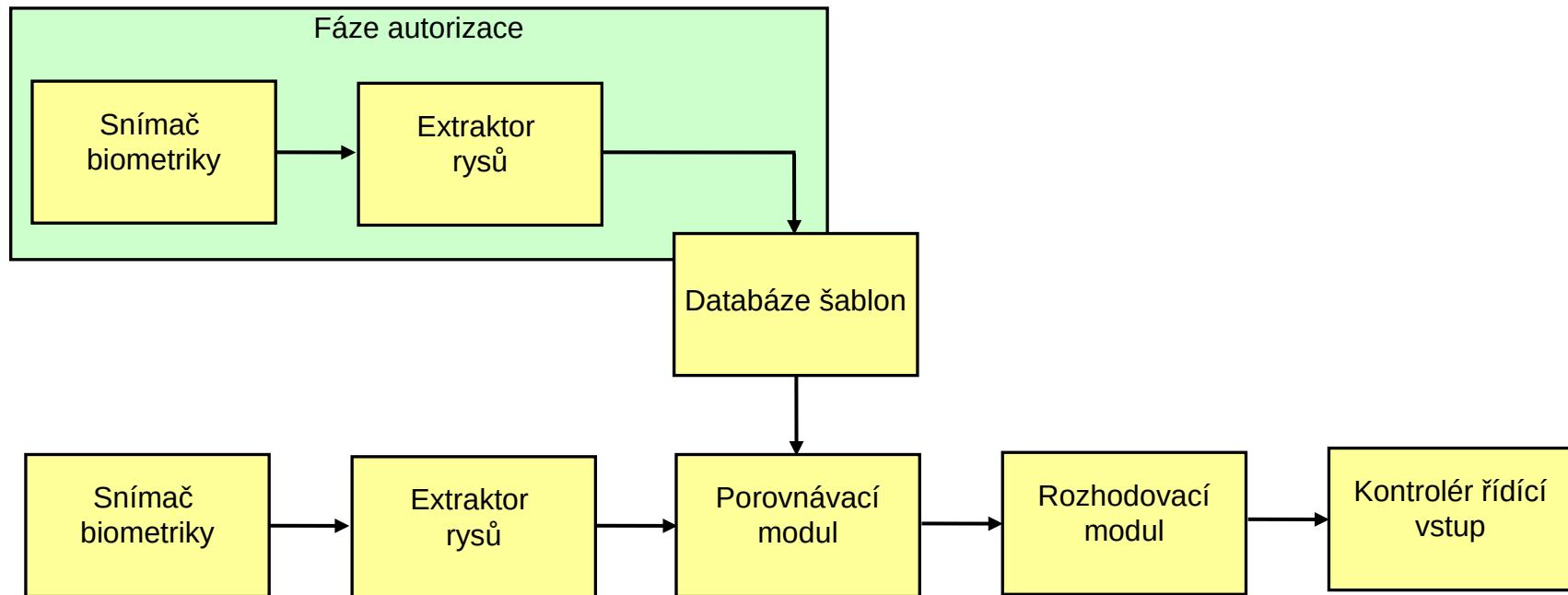
- V biometrických systémech EKV jsou z **historických** důvodů **kontroléry** obvykle spravovány přes **sběrnici RS-485**. Po této sběrnici jsou jim aktualizovány **přístupové seznamy**, tj. seznamy s identifikátory ID uživatelů a s jejich právy.
- V biometrických systémech **autentizaci** zpravidla provádějí **terminály** a těm je nutno distribuovat a aktualizovat **ověřovací seznamy**, tj. seznamy s ID uživatelů a jejich OF. Ke komunikaci mezi správní jednotkou a terminály se obvykle používá počítačová **IP síť**.



4. Vlastnosti biometrických autentizací

Schéma řízení přístupu s biometrickou autentizací

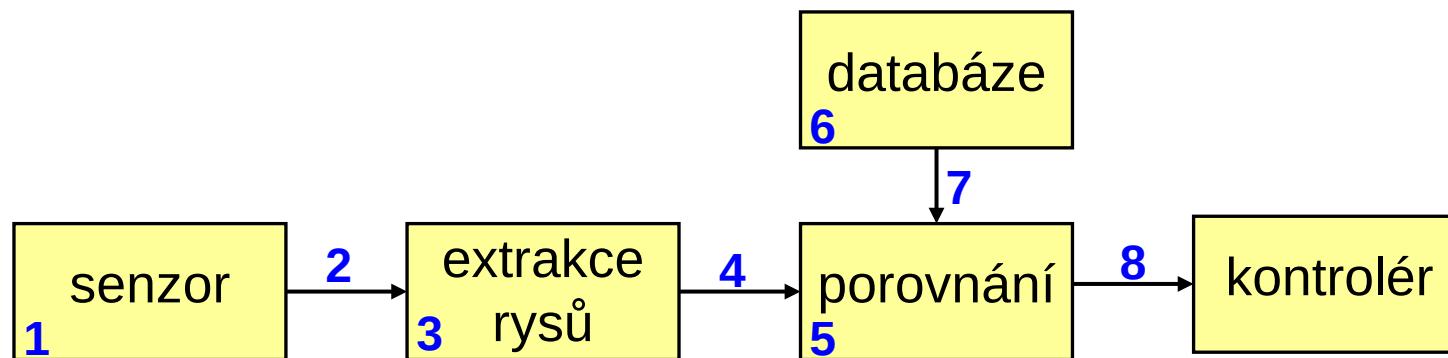
- Autorita ve fázi **autorizace** žadatele **sejme** jeho biometriku a **uloží** ji do databáze šablon.
- Při žádosti o přístup je biometrika žadatele opět **sejmota** a je **porovnána** se šablonou. V případě dostatečné shody je žadateli umožněn přístup.



Útoky na biometrickou autentizaci

- Možné útoky na systém biometrické autentizace:

1. podvrh biometrického objektu (např. model prstu),
2. opakování starých dokazovacích dat (tj. záznam z dřívější autentizace),
3. modifikace extraktoru (např. úprava programu),
4. opakování starých dat z extraktoru,
5. modifikace bloku porovnání,
6. modifikace záznamu v databázi,
7. modifikace přenášené šablony,
8. změna výsledku.

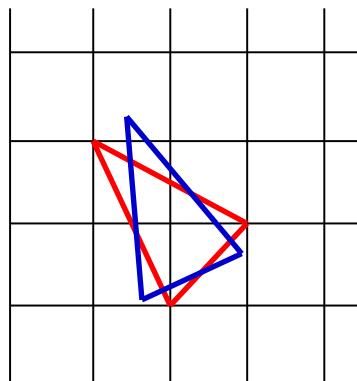


Statistické porovnávání biometrik

- Mějme aktuálně **sejmutou** biometriku vyjádřenu jako vektor $W = (w_1, w_2, \dots, w_n)$ a **šablonu** biometriky vyjádřenu jako $V = (v_1, v_2, \dots, v_n)$.
- K porovnání míry shody W a V se používají **různé** metriky.
- Příklad metriky **Similarity**: $s = S(W, V) = (W \cdot V) / (A \cdot B)$, kde

$$W \cdot V = \sum_{i=1}^n w_i \cdot v_i \quad A = \sqrt{\sum_{i=1}^n w_i \cdot w_i} \quad B = \sqrt{\sum_{i=1}^n v_i \cdot v_i}$$

- Pro tuto metriku platí, že $S = 1$, když $W = V$. Čím jsou si W a V podobnější, tak S se více blíží 1.
- Příklad: $W = [1,00; 3,00; 2,00; 1,00; 3,00; 2,00]$ a $V = [1,41; 3,28; 1,66; 1,08; 2,94; 1,66]$. Potom $W \cdot V = 27,79$, $A = 5,2915$ a $B = 5,2979$. Míra shody $s = 0,9913$, což je velmi blízké 1, takže lze konstatovat, že W a V si jsou velmi podobné.

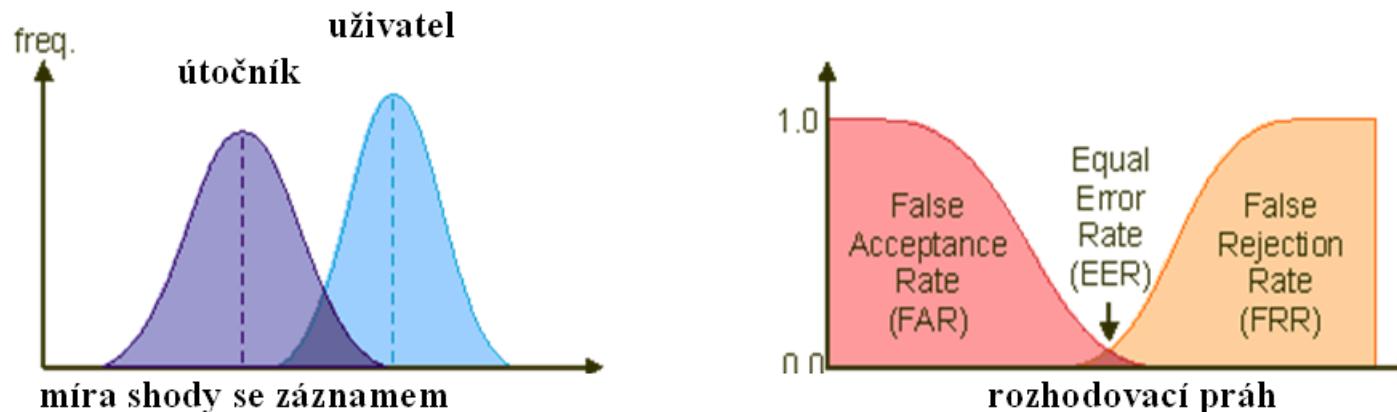


Zadání výše uvedeného příkladu odpovídá obrázku vlevo.
Vrcholy trojúhelníku jsou přitom pozice odpovídajících markantů otisku prstu.

Červený trojúhelník vznikl z OF a **modrý** odpovídá DD. Prakticky jde o to, že žadatel oproti autorizaci pootočil prstem o **20°**.

Přesnost biometrických metod

- Přesnost biometrických metod autentizace se hodnotí pomocí dvou parametrů:
 - pravděpodobnost chybného odmítnutí **FRR** („False rejection rate“), tj. je odmítnut přístup oprávněné osobě,
 - pravděpodobnost chybného povolení **FAR** („False acceptance rate“), tj. je povolen přístup neoprávněné osobě.



parametr \ charakteristika	otisk prstu	obličej	oční duhovka
FRR	0,2 – 36 %	3,3 – 70 %	1,9 – 6 %
FAR	0 – 8 %	0,3 – 5 %	1 % <
doba autentizace	9 – 19 s	10 s	12 s
objem záznamu	250 – 1000 B	84 – 1300 B	512 B

Zhodnocení biometrického zabezpečení

Výhody:

- Biometriku má osoba stále s **sebou**.
- Moderní metody preferují uživatelsky **přátelské** autentizace.

Nevýhody:

- Biometrické zabezpečení je obvykle **drahé**.
- Biometrická autentizace **není jednoznačná**. Aktuálně změřená biometrika zpravidla není stejná jako při autorizaci (např. tlak prstu na snímač, nečistoty na prstu apod.). Musí se tak akceptovat nenulové hodnoty FAR a FRR.
- Biometrika obecně **není tajná**. Takže kdo dokáže **napodobit** biometriku se může vydávat za oprávněnou osobu.

5. Elektronické a mechanické zabezpečení

Sjednocující pohled na elektronické a mechanické zabezpečení

- Bezpečnost aktiv spočívá jak na jejich **elektronickém** zabezpečení (např. použitém PZS, EKV atd.), tak i na jejich **mechanickém** zabezpečení (použité dveře, okna, zámky atd.).
- V současné době **neexistují** standardy, které by elektronické i mechanické zabezpečení aktiv řešily ve vzájemných souvislostech a proporcionálně.
- První takovou vlaštovkou v ČR je **doporučení** „Stanovení úrovně zabezpečení objektů a provozoven proti vloupání podle evropských technických norem“, které obsahuje návrh přiřazení stupňů mechanického zabezpečení a stupňů zabezpečení PZS.
- Stupeň zabezpečení PZS definuje standard **ČSN CLC/TS 50131** („Poplachové systémy – Poplachové zabezpečovací a tísňové systémy – Část 1: Systémové požadavky“). V něm jsou stanoveny **1. až 4. stupeň** zabezpečení. Ty již známe z 2. přednášky.
- Mechanické zabezpečení řeší standard **ČSN EN 1627** („Dveře, okna, lehké obvodové pláště, mříže a okenice – Odolnost proti vloupání – Požadavky a klasifikace“). V něm je definováno 6 stupňů odolnosti dveří a oken, které se označují jako **bezpečnostní třídy RC 1 až RC 6** („Resistance Class“). Každá třída stanovuje po jakou dobu má daný prvek odolávat průniku útočníka s definovaným vybavením a zkušenostmi. Například prvek třídy RC 3 má vzdorovat minimálně 5 minut útočníkovi, který je vybaven páčidlem o délce 710 mm, šroubovákem a dalším ručním nářadím, jako je malé kladivo, důlčíky a mechanická ruční vrtačka.

Tabulka adekvátních zabezpečení

- Níže uvedená tabulka popisuje **adekvátní** mechanické a poplachové zabezpečení pro stupně poplachového zabezpečení 1 a 2.
- **Uzamykacím systémem** se rozumí kombinace zámku, vložky a kování. Odolnost těchto systémů vůči průniku (označuje se jako typy 1 až 5) stanovuje v ČR svými certifikáty Národní bezpečnostní úřad (**NBÚ**).
- Odolnost **skleněných výplní** stanovuje norma **ČSN EN 536**. Pro vloupání definuje třídy P6B, P7B a P8B. Například skleněná výplň třídy P6B musí vydržet 30 až 50 úderů standardizovanou sekerou. Takováto výplň bývá z vrstveného skla o tloušťce cca 15 mm.
- Pokud tedy analýzou rizik dojdeme například k závěru, že pro daný objekt by PZS měl být 2. stupně zabezpečení, tak by zároveň bylo vhodné, aby tento objekt měl venkovní okna a dveře třídy RC 4, uzamykací systémy typu 3 a skleněné výplně třídy P7B.

Prvek mechanického zabezpečení	1. stupeň PZS	2. stupeň PZS
Okna a vchodové dveře	RC 3	RC 4
Uzamykací systém	typ 2	typ 3
Skleněné výplně	P6B	P7B

6. Závěr

Závěr

- Biometrické zabezpečení je v současné době velmi **různorodé**. Každá metoda má své výhody, ale i nevýhody.
- Zatím však lze konstatovat, že používané metody jsou buď **drahé**, nebo **málo** spolehlivé.
- Trendem je proto použití více metod najednou nebo jejich kombinace s jinými autentizačními metodami (tzv. **vícefaktorová autentizace**).
- V praxi se často využívá **dvoufaktorová** autentizace, kdy se žadatel zpravidla autentizuje předmětem (např. kartou) a znalostí (např. heslem pro aktivaci karty).
- **Třífaktorová** autentizace sestává z kombinace všech tří tříd autentizace – tj. předmětem, biometrikou i znalostí (např. USB token s vestavěnou čtečkou otisků prstů a PINem).
- Otázka ke zkoušce:
Biometrické přístupové systémy:
 - Architektura a správa biometrického systému EKV.
 - Otisky prstů – princip a vlastnosti.
 - Cévní řečiště prstu a dlaně – princip a vlastnosti.
 - Obličej – princip a vlastnosti.
 - Duhovka – princip a vlastnosti.